



Comments to BEREC's Draft Guidelines on Net Neutrality

July 17, 2016

Table of Contents

Executive Summary	3
Introduction	4
Background and General Aspects	5
General comments	5
Specific comments on terminology	5
Subject matter and scope	7
Specific comments to Article 1	7
Definitions	8
General Comments	8
Detailed comments to Article 2	8
Rights of End users and Commercial Practices	10
General comments	10
Detailed comments to Article 3(1)	10
Detailed comments to Article 3(2)	10
Traffic Management	14
Detailed comments to Article 3(3) first subparagraph	14
Detailed comments to Article 3(3) second subparagraph	14
Services other than IAS	18
General comments	18
Detailed comments to Article 3(5) first paragraph	18
Detailed comments to Article 3(5) second subparagraph	24
Transparency measures	29
General comments	29
Detailed comments to Article 4(1) letter d	29

Executive Summary

Telenor welcomes the opportunity to comment on the draft BEREC guidelines. While we appreciate the 6 week consultation period the process leading up to the publication of the draft guidelines with very limited exchange with industry is regrettable. Having had the opportunity to review the draft guidelines it is clear that a more open approach could have benefitted the process. Of particular concern is the lack of clarity in the draft guidelines. Telenor's main concerns are the following:

- In several areas the draft guidelines go beyond the mandate given to BEREC by the Regulation which is to "issue guidelines for the implementation of the obligations of national regulatory authorities". While we appreciate that BEREC must interpret the Regulation when crafting guidelines there are limits to BEREC's remit in this regard. Prohibiting per se some commercial offers instead of a case per case approach for example is not in line with the Regulation.
- The draft guidelines adopt a rigid and static interpretation of networks and service. An example is the considerations related to VPN. The draft guidelines are backward-looking and fail to consider the impact of network evolutions like SDN/NFV. It is important that NRAs through use of the guidelines do not prevent EU operators from remaining competitive and from implementing networks and services for the future.
- The process and requirements of the case-by-case approach for evaluation of commercial practices as set out in the draft guidelines are far reaching and have an unclear basis in competition law principles. Uncertainty is also created as to whether NRAs monitoring is only ex post. An ex-ante type of approach to commercial practices, which pre-defines how companies develop offers, set prices and sell services, would have a devastating effect on the development of the market. Moreover, this will be directly contrary to deregulation of the retail market that has occurred as fully supported by ex-ante market analysis. The Telecom Regulatory Framework and competition law is fully equipped to deal with any problems which commercial practices could present.
- Co-legislators decided not to define and not to regulate specialised services, but the draft guidelines opt for an opposite approach. Also the draft guidelines appear to reverse the burden of proof: it is clear from the Regulation that NRAs are to show when a given practice is not be in line with the Regulation. Furthermore, the Regulation does not mandate the kind of "two lane approach" as BEREC seems to do regarding what services should be allowed and what should not. BEREC is apparently of the view that there can be only two kinds of internet access, either IAS or what BEREC refers to as Specialised Services. This approach is erroneous and puts EU innovation at risk, as Telenor argues in this response.
- Reasonable traffic management is necessary and should not be opposed to investment that remains operators' decision. BEREC erroneously considers that more investments in capacity would be the best answer in all cases to traffic management; for instance the latency needs cannot be addressed simply by adding more capacity.

In our view, the draft guidelines need to be significantly revised: Key sections are inappropriately restrictive, call for NRA assessments and intervention without proper justifications and go beyond the purpose of the Regulation in several instances. As currently formulated the guidelines do not create the legal certainty required for operators in order to make investment decisions and may ultimately result in harm to consumers through stifled innovation and lack of choice.

Introduction

Detailed comments to the draft BEREC guidelines on Net Neutrality are set out in the following.

Our response follows the same structure through-out. First we state the guideline paragraph(s) in question followed by our commentary to the specific paragraph(s). Paragraphs of the BEREC draft guidelines are mentioned as “§X”. For instance, “§15” refers to paragraph 15 of BEREC draft guidelines.

We discuss the following sections of the guideline in turn:

- Background and General Aspects
- Subject Matter and Scope
- Definitions
- Rights of End users and Commercial Practices
- Traffic Management
- Services other than IAS
- Transparency Measures

Background and General Aspects

General comments

Article 1 states that the subject matter and scope of the Regulation is: “... to safeguard equal and non-discriminatory treatment of traffic in the provision of internet access services ...” Therefore, the text for which BEREC must adopt guidelines in order to ensure a harmonised interpretation in Europe should refer to “open internet access” and not to “net neutrality”. There exists no formally accepted definition of net neutrality.

We suggest that the guidelines be termed “BEREC Guidelines on the Application by National Regulators of European Open Internet Access Regulation”

Specific comments on terminology

§2. For the purpose of these Guidelines, BEREC has used the following terms throughout the Guidelines to improve readability.

Application	In these Guidelines, BEREC use the term “application” as a short expression for more lengthy expressions from the Regulation, like “applications and services”, “content, application and service”. In the choice of using “application” or “service”, BEREC finds that “application” is better to distinguish from the underlying electronic communication service which on the other hand can be referred to as a “service”.
CAP (Content and Application Provider)	CAPs make content (e.g. web pages, blogs, video) and/or applications (e.g. search engines, VoIP applications) and/or services available on the Internet. CAPs may also make content, services and applications available via specialised services.
ISP (Internet Service Provider)	In these Guidelines, BEREC uses the term “ISP” to refer to providers of internet access services (IAS). ISPs may also be providers of specialised services.
Specialised service	In these Guidelines, BEREC uses the term “specialised services” as a short expression for “services other than internet access services which are optimised for specific content, applications or services, or a combination thereof, where the optimisation is necessary in order to meet requirements of the content, applications or services for a specific level of quality” (ref. Article 3(5)).

In §2 BEREC refers to content, application and services provided on top of the network as “application” while using the term “service” for the underlying electronic communication service. This terminology is not consistent with the Regulation and BEREC is not using definitions consistently. As an example, consider §22 where it is stated that an end user has the right to use and provide applications and services. According to §2 “service” means “electronic communications service” and contrast it with §4 stating that according to the Framework Directive an end-user is someone not providing electronic communications services.

Further, by making this distinction, BEREC implies that all “applications” are provided by OTTs and deserve protection while ISP services must abide by the rules set by the Regulation. This definition does therefore not take into account the possibility for an ISP to also supply “applications” or indeed that the ISP is also a CAP. The misunderstanding might lie in the reference to the underlying “electronic communication service” in the definition instead of to the underlying IAS.

Subject matter and scope

Specific comments to Article 1

§5. CAPs are protected under the Regulation in so far as they use an IAS to reach other end-users. However, some CAPs may also operate their own networks and, as part of that, have interconnection agreements with ISPs; the provision of interconnection is a distinct service from the provision of IAS.

§6. NRAs may take into account the interconnection policies and practices of ISPs in so far as they have the effect of limiting the exercise end-user rights under Article 3(1). For example, this may be relevant in some cases, such as if the interconnection is implemented in a way which seeks to circumvent the Regulation.

According to §6 BEREC holds the view that NRAs have a mandate to intervene in the interconnection policies and practices of ISPs. Telenor disagrees with this interpretation of the Regulation for the following reasons.

The subject matter of the Regulation concerns *“equal and non-discriminatory treatment of traffic in the provision of internet access services and related end-users’ rights”*, and does not extend to IP interconnection practices or agreements.

BEREC’s justification relies on a misinterpretation of the term “commercial practices” in Article 3(2) and Recital (7) of the Regulation. The objective of the said article and recital is to enshrine the freedom of ISPs and end-users to agree on the technical and commercial conditions and characteristics of the IAS and to subject commercial practices used between the same parties (i.e. ISPs and end-users) in connection with the retailing of internet access services to certain limitations.

Commercial practices are defined by the Unfair Commercial Practices Directive as *“any act, omission, course of conduct or representation, commercial communication including advertising and marketing, by a trader, directly connected with the promotion, sale or supply of a product to consumers”*. This definition clarifies that commercial practices should be understood as unilateral activities of ISPs related to the retailing of IAS services to end-users. The term needs to be interpreted in the context of the article in which it is used, which prevents it from being extended to cover IP interconnect agreements.

Finally, the term ‘commercial practices’ was introduced into the Regulation as a compromise afforded to Member States intending to regulate zero-rating. At no point in the legislative process was the term intended to include IP interconnect.

We note that BEREC in §47 excludes IP interconnection practices from the scope of Article 3(3) first subparagraph. In our view IP interconnection is excluded from the scope of the entire Regulation.

Definitions

General Comments

The BEREC guidelines should stick to the definitions covered by the Regulation. The Regulation defines IAS, BEREC should therefore avoid using the term specialised services or using criteria that were disregarded by the co-legislators.

Detailed comments to Article 2

§11. Regarding virtual private networks (VPN) network services, these are typically provided by the ISP to anyone that wishes to enter a contract about the provision of such a service, and these would therefore typically be considered to be publicly available. The term 'private' describes the use of such a service which is usually limited to endpoints of the business entering the contract and is secured for internal communications. In accordance with Recital 17, to the extent that VPNs provide access to the internet, they are not a closed user group and should therefore be considered as publicly available ECS and are subject to Articles 3(1)-(4). VPNs are further discussed in paragraph 111.

BEREC states that VPN services are typically publicly available, and draws the conclusion that they are subject to Articles 3(1)-(4). However, elsewhere in the guidelines (see §111) it is suggested that VPN services have optimized levels of quality and therefore constitute "Specialised services" for which Articles 3(1)-(4) do not directly apply. §11 should be amended or deleted.

§17. BEREC understands a sub-internet service to be a service which restricts access to services or applications (e.g. banning the use of VoIP or video streaming) or enables access to only a pre-defined part of the internet (e.g. access only to particular websites). NRAs should take into account the fact that an ISP could easily circumvent the Regulation by providing such sub-internet offers. These services should therefore be considered to be in the scope of the Regulation and the fact that they provide a limited access to the internet should constitute an infringement of Articles 3(1), 3(2) and 3(3) of the Regulation. BEREC refers to these service offers as 'sub-internet services', as further discussed in paragraphs 35 and 52.

The Regulation does not define the concept of "sub internet" services. The BEREC definition of sub-internet services and the conclusion that they constitute an infringement of the Regulation lacks legal support in the Regulation. Further, BEREC's suggested definition is not clear. This is problematic for the provision of both existing services and new and innovative services. As an example consider add-ons provided by Telenor Bulgaria: 1GB for use only for Facebook. It is not clear whether BEREC would consider this to be an "add-on" to an IAS or as separate "sub-internet" service.

This guideline also risks creating a discriminatory situation where limited access for "device-based" offers would be permitted but not "access-based". Users, in particular businesses, should be allowed to contract any kind of IAS access that serves their requirements and even to request blockage of certain categories of traffic and/or protocols. They should not be forced to purchase specialised devices to get the IAS access they demand (ref. below); thus this draft guideline should be deleted.

§18. Services where the number of reachable end-points is limited by the nature of the terminal equipment used with such services (e.g. services designed for communication with individual devices,

such as e-book readers as well as machine-to-machine devices like smart meters etc.) are considered to be outside the scope of the Regulation unless they are used to circumvent this Regulation. They could use an IAS (but not provide an IAS nor constitute a substitute to an IAS), use a private network or constitute a specialised service. If these services are using an IAS or constitute a specialised service the connectivity service will be subject to the relevant rules applicable to IAS and specialised services in the Regulation.

§18 starts out by stating that “services where the number of reachable end-points is limited by the nature of the terminal equipment used with such services” are outside scope. However, such a “service” will use IAS, a specialised service or a private network for connectivity. According to the same paragraph, both IAS and specialised services are covered by the regulation. Thus the connectivity part of the service is only outside scope in the private network case. Such services are outside scope anyway (ref. §9). Further, terminals are outside scope (ref. §51). In conclusion, it seems §18 is unnecessary.

Rights of End users and Commercial Practices

General comments

The Regulation states that commercial offers shall not limit the exercise of the rights of end users (Article 3(2)) and Recital 7 does mention that an ex post case by case assessment of certain agreements and commercial practices based on criteria such as the parties market positions should be undertaken. However, on many aspects, BEREC adopts a more restrictive approach than the Regulation by prohibiting some commercial offers per se and by expanding on the assessment criteria. Telenor recalls that price differentiation is a different subject matter than discrimination of traffic (e.g. blocking, throttling). Zero rated offers can be seen as a form of price differentiation. In terms of the Regulation a ban on price differentiation is clearly not within scope; nor should it be in the BEREC guidelines.

Detailed comments to Article 3(1)

§23. Thirdly, end-users have the right to use terminal equipment of their choice. Directive 2008/63/EC defines “terminal equipment” as “equipment directly or indirectly connected to the interface of a public telecommunication network”. The right to choose terminal equipment therefore covers equipment which connects to the interface of the public telecommunications network. This interface, the network termination point (NTP), is defined in Article 2 letter (da) of the Framework Directive (2002/21/EC), meaning the physical point at which a subscriber is provided with access to a public communications network.

The BEREC guidelines should make clear that terminal equipment must comply with the interfaces of public networks which network operators have then the obligation to publish under EU law (Radio Equipment DIRECTIVE 2014/53/UE).

§25. Moreover, NRAs should consider whether there is an objective technological necessity for the obligatory equipment to be considered as part of the ISP network. If there is not, and if the choice of terminal equipment is limited, the practice would be in conflict with the Regulation. For example, the practice of restricting tethering⁹ is likely to constitute a restriction on choice of terminal equipment because ISPs “should not impose restrictions on the use of terminal equipment connecting to the network in addition to those imposed by manufacturers or distributors of terminal equipment in accordance with Union law” (Recital 5).

The BEREC draft guidelines consider that the practice of restricting tethering is likely to constitute a restriction in breach of the Regulation but this is not explicit from the Regulation. A more proportionate approach should be taken as such a prohibition risks jeopardising innovation for IAS providers, with risks on unlimited data offers.

Detailed comments to Article 3(2)

§38. A zero-rating offer where all applications are blocked (or slowed down) once the data cap is reached except for the zero-rated application(s) would infringe Article 3(3) first (and third) subparagraph (see paragraph 52).

The per se ban on a zero-rating offer where all applications are blocked once the data cap is reached except for the zero rated application(s), is an example of discrimination of traffic. BEREC provides clarification that such practice would infringe the Regulation. The draft Guidelines omit to highlight that such type of offers can also benefit the end users; for instance such services can be used to provide customers with an opportunity to trial new services or to enjoy ancillary services like IAS providers' customer care, speed tests etc. Further, looking forward, voice calls will increasingly be delivered as data calls, in this regard calls to emergency services should not be prevented as a result of a data cap being in place.

Operators should be able to innovate and explore different business models under a case by case ex post monitoring by the NRA as foreseen by the Regulation. There should be no default prohibition of a zero rated offer and hence §38 should be deleted. However, in the event this guideline is retained, Telenor suggests that BEREC a priori exempt ancillary services like IAS' customer care, speed tests, distress calls etc. By allowing for these narrowly defined services, when other traffic is blocked, does not pose a threat to the rights of end users. Moreover, this does not impact end-users or any service provider negatively. For example, the IAS' customer care can only be offered by the ISP itself.

§39. The ISP could either apply or offer zero-rating to an entire category of applications (e.g. all video or all music streaming applications) or only to certain applications thereof (e.g. its own services, one specific social media application, the most popular video or music applications). In the latter case, an end-user is not prevented from using other music applications. However, the zero price applied to the data traffic of the zero-rated music application (and the fact that the data traffic of the zero-rated music application does not count towards any data cap in place on the IAS) creates an economic incentive to use that music application instead of competing ones. The effects of such a practice applied to a specific application are more likely to "undermine the essence of the end-users' rights" or lead to circumstances where "end-users' choice is materially reduced in practice" (Recital 7) than when it is applied to an entire category of applications.

While price differentiation can be problematic under certain conditions, this needs to be proved. The (retail) market in Europe is competitive and end-users can choose between subscriptions and data packs offered by competing MNOs. Competition law would apply also to zero rating and/or internet access providers and would in our view be sufficient should any problems arise.

There is no explicit mention of zero rating in the Regulation. BEREC draft guidelines are therefore going beyond the Regulation. Further, the analysis presented in the guidelines is flawed. A lower price does not restrict consumer choice. A lower price will to the contrary ease the budget constraint of the consumers. The wording used also underlines that BEREC's interpretation here is flawed. *Materially* and *in practice* points to a high threshold. Price fluctuations are everyday events. Only prohibitively large price increases would normally be considered to reduce consumer choice in a material way.

BEREC should advise NRA's to adopt an enforcement strategy which is very closely aligned to an ex post approach (competition law). To avoid the risk of over-regulation competition principles must serve as the basis for the assessment of the compatibility of such practices under the TSM Regulation.

§43. In light of the aforementioned considerations, BEREC considers that a comprehensive assessment of such commercial and technical conditions may be required, taking into account in particular:

- the goals of the Regulation and whether the relevant agreements and/or commercial practices circumvent these general aims;
- the market positions of the ISPs and CAPs involved - a limitation of the exercise of end-user rights is more likely to arise where an ISP or a CAP has a 'strong' market position (all else being equal) compared to a situation where the ISP or CAP has a 'weak' market position. The market positions should be analysed in line with competition law principles;
- the effects on consumer and business customer end-user rights, which encompasses an assessment of inter alia:
 - whether there is an effect on the range and diversity of content and applications which consumer end-users may use and, if so, whether the range and diversity of applications which end-users can choose from is reduced in practice;
 - whether the end-user is incentivised to use, for example, certain applications;
 - whether the IAS subscription contains characteristics which materially reduce end-user choice (see in more detail in paragraph 45).
- the effects on CAP end-user rights, which encompasses an assessment of, inter alia:
 - whether there is an effect on the range and diversity of content and applications which CAPs provide, and to what extent the range and diversity of applications may not be effectively accessed;
 - whether CAPs are materially discouraged from entering the market or forced to leave the market, or whether there are other material harms to competition in the market concerned (see in more detail in the fourth bullet of paragraph 45 with regard to offers);
 - whether the continued functioning of the internet ecosystem as an engine of innovation is impacted, for example, whether it is the ISP that picks winners and losers, and on the administrative and/or technical barriers for CAPs to enter into agreements with ISPs.
- the scale of the practice and the presence of alternatives - a practice is more likely to limit the exercise of end-user rights in a situation where, for example, many end-users are concerned and/or there are few alternative offers and/or competing ISPs for the end-users to choose from;
- the effect on freedom of expression and media pluralism (ref. Recital 13).

45. In applying such a comprehensive assessment, NRAs and other competent authorities may also take into account the following considerations:

- Any agreements or practices which have an effect similar to technical blocking of access (see paragraph 52) are likely to infringe Articles 3(1) and 3(2), given their strong impact on end-user rights.
- Commercial practices which apply a *higher* price to the data associated with a specific application or class of applications are likely to limit the exercise of end-users' rights because of the potentially strong disincentive created to the use of the application(s) affected, and consequent restriction of choice. Also, the possibility that higher prices may be applied to an application or category of application may discourage the development of new applications.

- End-users of an IAS whose conditions include a lower (or zero) price for the data associated with a specific application or class of applications will be incentivised to use the zero-rated application or category of applications and not others. Furthermore, the lower the data cap, the stronger such influence is likely to be.
- Price differentiation between *individual* applications within a category has an impact on competition between providers in that class. It may therefore be more likely to impact the “*continued functioning of the internet ecosystem as an engine of innovation*” and thereby undermine the goals of the Regulation than would price differentiation between *classes* of application.

The assessment criteria mentioned by BEREC in §43 and §45 are unfortunately biased in the sense that they artificially construct theories of market failure. This is too simplistic, impractical and raises significant risk that a Type I error¹ could occur in the NRA assessments. As an example of impracticality consider that NRAs are to assess the market position of ISPs and CAPS and Über is zero-rated. This could mean that the market for taxi services would need to be assessed by NRAs. This is clearly out of scope.

Where a given NRA considers there might be an issue with a commercial offer, it should check whether the conditions mentioned in Recital 7 are fulfilled, namely does the commercial offer materially reduce the choice of the end users in practice, taking into account the market position of the IAS and CAP providers and does it undermine the essence of the end users rights.

Additionally, openness should be a key point for NRAs assessing a commercial practice concerning IAS. If all CAPs have the same rights and ability to conclude commercial agreements with ISPs, then the practice should be considered as compliant with the Regulation. This is for instance the case of “sponsored data” offers, which are proposed to all CAPs and through which IAS traffic is paid by the CAP rather than by end-users. Such offers are similar to “0800” services for telephone, or to “transport paid” postal services which no one has ever criticised for being non neutral. Such offers should be supported without reservation by BEREC guidelines.

¹ A type I error is the incorrect rejection of a true null hypothesis (a “false positive”, i.e., accepting a false hypothesis as correct).

Traffic Management

Detailed comments to Article 3(3) first subparagraph

§46. A basic principle of the Regulation relates to traffic management and is the obligation on ISPs to treat all traffic equally when providing IAS. Typically, infringements of this principle which are not justified according to Article 3(3) would also constitute an infringement of the end-user rights set out in Article 3(1).

Article 3 (2) of the regulation reflects that IAS can have different technical conditions and characteristics “[...] such as price, data volumes or speed [...] provided that these do not limit the exercise of the end-user rights in Article 3(1). Thus, the Regulation explicitly supports the ability for ISP to segment IAS by technical characteristics such as in terms of speeds and volumes. This segmentation may involve quality differentiation between individual accesses and subscriptions so end users can choose the IAS that best fits their needs, e.g. a subscription with low latency for gaming or a subscription with high speed and high data volume for video. Therefore, NRAs should include in their analysis of non-discrimination the freedom for ISP to segment the quality between IAS offers provided to different end-users and answering different needs.

Moreover, The Regulation does not impose specific rules concerning management of traffic concerning two different end-users’ accesses. Any rigid rule on how network resources should be allocated between different end-users using IAS services of different quality or speed would go beyond the provisions of the Regulation and lead to inefficient and arbitrary outcomes.

The guidelines must not prohibit traffic management required for offering different customers IAS with service characteristics that meet their needs.

§50. NRAs should take into account that equal treatment does not necessarily imply that all end-users will experience the same network performance or quality of service (QoS). Thus, even though packets can experience varying transmission performance (e.g. on parameters such as latency or jitter), packets can normally be considered to be treated equally as long as all packets are processed agnostic to sender and receiver, to the content accessed or distributed, and to the application or service used or provided.

The Regulation provides that reasonable traffic management is permitted and also recognises that it contributes to the efficient use of network resources and optimisation of overall quality. While the Regulation focuses on the technical needs of the traffic, the draft guidelines go further in §50 and provide that “packets can normally be considered to be treated equally as long as all packets are processed agnostic to sender and receiver, to the content accessed or distributed, and to the application or service used or provided”. Traffic today and even more so in a 5G world will have different needs and cannot be processed in a way that is completely “agnostic to sender and receiver, to the content accessed or distributed, and to the application or service used or provided”. See also our comments on traffic management below. This part of §50 should be deleted.

Detailed comments to Article 3(3) second subparagraph

§54. In assessing whether an ISP complies with the principle of equal treatment set out in Article 3(3) first subparagraph, NRAs should take into account whether a measure (which, prima facie, appears

to infringe this principle) is a reasonable traffic management measure. The principle of equal treatment of traffic does not prevent ISPs from implementing reasonable traffic management measures in compliance with Article 3(3) second subparagraph.

Article 3(3) of the Regulation provides that ISPs are free to technically optimise the IAS service they provide to their customers, on a competitive basis as long as they use reasonable traffic management as defined by the Regulation itself. Excessive regulatory interference in this domain would hurt the efficient management of IAS traffic, impede competition between providers and ultimately harm end-users.

The Regulation clearly acknowledges the need and right for operators to manage their networks. BEREC guidelines should therefore not include wording such as “prima facie appears to infringe this principles”. NRAs should be concerned by the outcomes of traffic management, not by monitoring the technical options chosen by each ISP to achieve these outcomes. Administrative interference should be avoided in order to keep operational traffic management efficient for the benefit of end-users.

§57. When considering whether a traffic management measure is non-discriminatory, NRAs should consider the following:

- The requirement for traffic management measures to be non-discriminatory does not preclude ISPs from implementing - in order to optimise the overall transmission quality and user experience - traffic management measures which differentiate between objectively different categories of traffic (ref. Recital 9 and paragraphs 59-64 below).
- Similar situations in terms of similar technical QoS requirements should receive similar treatment.
- Different situations in terms of objectively different technical QoS requirements can be treated in different ways if such treatment is objectively justified.
- In particular, the mere fact that network traffic is encrypted should not be deemed by NRAs to be an objective justification for different treatment by ISPs.

§61. Furthermore, as explained in Recital 9, ISPs’ traffic management measures are “*responding to*” the QoS requirements of the categories of traffic in order to optimise the overall transmission quality and enhance the user-experience. In order to identify categories of traffic, the ISP relies on the information provided by the application when packets are sent into the network. (See also paragraph 67 regarding which information can legitimately be considered by ISPs). Encrypted traffic should not be treated less favourably by reason of its encryption.

This draft guideline allows for differentiation on the basis of different technical quality of service requirements, but seems to go further than the regulation without adding clarity. If ISPs are to prioritize certain applications (set the same QoS requirement) there is a need to be able to identify those applications with 100% accuracy. This can be a problem if the traffic is encrypted and/or if ISPs do not have some sort of arrangement with the CAP/OTT provider (see also below).

Regardless of any effort of the ISP it is not possible to treat all traffic of the same category as seen from the end-users’ perspective. This is also reflected in §61: “In order to identify categories of

traffic, the ISP relies on the information provided by the application when packets are sent into the network". CAPs decide what protocols their services are using and whether they use end-to-end encryption. Finally, it must be acknowledged that, the objective of not treating encrypted traffic less favourably by reason of its encryption is in reality not technically possible with 100% accuracy.

§63. Based on this, reasonable traffic management may be applied to differentiate between objectively different "categories of traffic", for example by reference to an application layer protocol (such as SMTP, HTTP or SIP) or generic application types (such as file sharing, VoIP or instant messaging), only in so far as:

- the application layer protocol or generic application type are linked to objectively different technical QoS requirements;
- applications with equivalent QoS requirements are handled agnostically in the same traffic category; and
- justifications are specific to the objectives that are pursued by implementing traffic management measures based on different categories of traffic.

§67. Conversely, traffic management measures that monitor aspects other than the specific content, i.e. the generic content, should be deemed to be allowed. Monitoring techniques used by ISPs which rely on the information contained in the IP packet header, and transport layer protocol header (e.g. TCP) may be deemed generic content, as opposed to the specific content provided by end-users themselves (such as text, pictures and video).

§67 seems to assume that information other than in IP-headers and transport layer protocol header may be deemed as specific content provided by the end-users, while §63 refers to application layer protocols, but only lists transport layer and below.

It should be noted that ISPs might use DPI for traffic management purposes. DPI is used to classify application layer protocols, and with encryption heuristic methods may be necessary for this classification (not 100% accuracy in such case).² The draft guidelines are in our view unclear on this point, and we must emphasize that ISPs may need to look beyond transport layer protocol headers to be able to classify the traffic, but without revealing any user content.

§89. NRAs should monitor that ISPs properly dimension their network, and take into account the following:

- if there is recurrent and more long-lasting network congestion in an ISP's network, the ISP cannot invoke the exception of congestion management (ref. Recital 15);

² Obviously, the user payload will not be used, and any practice has to be in compliance with applicable (privacy) laws.

- application-specific congestion management should not be applied or accepted as a substitute for more structural solutions, such as expansion of network capacity.

This guideline implies that NRAs will get involved in the decisions of ISPs on how to dimension their networks. This is not proportionate and potentially intrusive into ISP operations and is not foreseen by the Regulation at all.

Services other than IAS

General comments

As an initial comment, Telenor draws attention to the primary intention of Article 3(5) first subparagraph and Recital 16, namely to secure that no Member State puts in place national legislation that forbids or complicates the provision of services other than IAS. However, if there is reason to believe that such services are in fact offered in a way that circumvent the key provisions regarding IAS traffic management, NRAs should according to the recital verify whether the optimization is objectively necessary.

In our view this should be interpreted as a basic freedom for providers of services, content and applications in the EU to offer Services Other than Internet Services, and NRA intervention should only be considered when there is a suspicion that such services are offered in order to circumvent the traffic management provisions in the Regulation.

Detailed comments to Article 3(5) first paragraph

§95. Beyond the delivery of a relatively high quality application through the IAS, there can be demand for a category of electronic communication services that need to be carried at a specific level of quality that cannot be assured by the standard best effort delivery.

While it is correct in most cases with today's networks that services, content and applications will be delivered over either best effort IAS or a dedicated connection over Internet where certain quality parameters have been optimized, it should be recognized that there also must be room for other forms of connectivity that does not meet the criteria for IAS in Article 2(2), and at the same time are not optimized to meet a specific level of quality, at least not in terms of speed, latency, packet loss, etc.

For 5G and IoT applications in particular the traffic could be routed over the Internet but with network defined limitations in the number of end points that are connected. Indeed, the number of use cases that can be catered for within 5G networks will increase significantly compared to the situation today and any concrete characterisation will be increasingly difficult.³ It can in our view not be the intention of the Regulation to exclude the use of such Services Other than IAS. The guidelines should not forbid or by other means exclude such use, as this would seriously restrict the ability of EU providers of services, content and applications to innovate and deliver new services.

³ 5G is expected to support both existing and countless new use cases with a high variety of applications and variability of their performance attributes: From delay-sensitive video applications to ultra-low latency, from high speed entertainment applications in a vehicle to mobility on demand for connected objects, and from best effort applications to reliable and ultra-reliable ones such as health and safety. Furthermore, use cases will be delivered across a wide range of devices and across a fully heterogeneous environment.

§96. Such services can be offered by providers of electronic communications to the public (PECPs), including providers of internet access services (ISPs), and providers of content, applications and services (CAPs).

Please refer to previous comment on §95 regarding the scope and to §112 regarding the relationship between different categories of providers.

§97. These providers are free to offer services referred to in Article 3(5), which BEREC refers to as specialised services, only when various requirements are met. Article 3(5) provides the safeguards for the provisioning of specialised services which are characterised by the following features in Article 3 (5) first subparagraph:

- they are services other than IAS services;
- they are optimised for specific content, applications or services, or a combination thereof;
- the optimisation is objectively necessary in order to meet requirements for a specific level of quality.

There are only three reasons according to the Regulation for NRA intervention against Services Other than IAS. The first reason concerns Services Other than IAS that are offered with the intention to circumvent the traffic management provisions of the Regulation. If the NRA suspects that the main objective of the service is to circumvent the traffic management provisions, then the NRA should scrutinize the offering and intervene in a relevant manner when appropriate. The remaining two reasons for intervention are if a Service Other than IAS is offered as replacement for IAS or if it has detrimental effect on the availability or the general quality of IAS, which is dealt with in §112 – 121.

It should be stressed that there are no other reasons in the Regulation to intervene against Services Other than IAS. The “requirements” and “conditions” listed by BEREC in §97-98 seem to have been decoupled from these reasons, and they appear as restrictions in their own right. This is in our view not the intention of Article 3(5) first paragraph, which instead makes it clear that there is a freedom to provide Services Other than IAS. §97 must be redrafted accordingly, as to explicitly show that the “requirements” are to be used when the NRA is in the task of verifying whether a service suspected of circumventing the traffic management provisions in the Regulation is indeed a legitimate service. If there is no evidence of the service circumventing the Regulation, then the NRA should respect the freedom of providing such services as guaranteed by Article 3(5) first paragraph.

§98. Their provision is subject to a number of conditions in Article 3(5) second subparagraph, namely that:

- the network capacity is sufficient to provide the specialised service in addition to any IAS provided;
- specialised services are not usable or offered as a replacement for IAS;
- specialised services are not to the detriment of the availability or general quality of the IAS for end-users.

As noted in the comment to §97 there is no *raison d'être* for “requirements” and “conditions” without the necessary context of the legal grounds for these restrictions (namely to eliminate circumvention of the traffic management provisions, to secure that non-IAS are not offered as replacement for IAS or avoiding detrimental effects to the availability and general quality of IAS).

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

This is one explicit basis in the Regulation for NRA intervention against Services Other than IAS, i.e. an exception from the rule that providers are free to offer Services Other than IAS. As a guideline for the NRAs it does not contribute in any way and should be deleted.

§100. All these safeguards aim to ensure the continued availability and general quality of best effort IAS.

It is important that the guidelines do not violate or extend the scope of the Regulation. Article 3(5) first paragraph is first and foremost about EU harmonization and gives an explicit right for providers of services, content and applications to offer Services Other than those which the Regulation covers. In spite of the freedom provided, NRAs have the mandate to intervene against a service that does not constitute IAS if that service circumvents the provisions regarding traffic management in the Regulation.

It is not clear what BEREC refers to with “All these safeguards”. The article specifies that the freedom is about optimized services where the optimization is necessary to meet the requirements for a specific level of quality. The recital mentions only one reason for intervention, i.e. if there is suspicion of the service circumventing the provision regarding traffic management then NRAs should verify the objective necessity of the optimization taking place. If the service is found to violate the Regulation then the NRA can intervene in accordance with Article 5(1) taking into account the need for effectiveness, necessity and proportionality (see §177).

§101. NRAs should “verify” whether the application could be provided over IAS at the agreed and committed level of quality, and whether the requirements are plausible in relation to the application, or whether they are instead set up in order to circumvent the provisions regarding traffic management measures applicable to IAS, which would not be allowed.

§102. Initially, the requirement of an application is set by the provider of the specialised service, although requirements may also be inherent to the application itself. For example, a video application could use standard definition with a low bitrate or ultra-high definition with high bitrate, and these will obviously have different QoS requirements. A typical example of inherent requirements is low latency for real-time applications.

§103. When assessing whether the practices used to provide specialised services comply with Article 3(5) first subparagraph, NRAs should apply the approach set out in paragraphs 104-111).

As stated above, the NRAs task of verifying the necessity of the optimization taking place according to Article 3(5) first subparagraph should be spurred by a suspicion of the service observed circumventing the provisions regarding traffic management. Such verification should be made case by case. It should be made clear in the guidelines that the mere fact that some of the optimized quality parameters are not strictly needed to deliver the service, should not by itself lead to the conclusion that the service is circumventing the Regulation.

Further Article 3(5) first paragraph does not call for an ex-ante assessment of all optimized services in the marketplace, which the draft guideline seems to suggest. It should therefore be stated clearly

that the guidance relating to NRA assessment is applicable when an NRA is set with the task of verifying the objective necessity of optimization ex-post, in a case of suspected circumvention of the Regulation. Then the inherent requirements of the services could be matched by the actual optimization taking place. If however there is no evidence of circumvention of the traffic management provisions, then the optimized services does not necessarily have to have characteristics with perfect match to the “inherent” requirements of the relevant service, content or application.

§104. NRAs could request from the provider relevant information about their specialised services, using powers conferred by Article 5(2). In their responses, the provider should give information about their specialised services, including what the relevant QoS requirements are (e.g. latency, jitter and packet loss), and any contractual requirements. Furthermore, the “specific level of quality” should be specified, and it should be demonstrated that this specific level of quality cannot be assured over the IAS.

104. The NRA should always be clear with the legal grounds for any intervention. If information is requested it should be explained why the information is needed (e.g. there is suspicion that the service is provided primarily to circumvent the traffic management provisions that would otherwise apply).

§105. Based on this information, the NRA should assess the requirements mentioned in Article 3(5) first subparagraph.

105. Any assessment should be based on the legal grounds for intervention. The Regulation does not call for mass surveillance of all services provided. Requests for information and assessments of services should instead follow from case-by-case investigations of suspected circumvention of the provisions in the Regulation. See comments to §102-103.

§106. If assurance of a specific level of quality is objectively necessary, this cannot be provided by simply granting general priority over comparable content. It is understood that specialised services are offered through a connection that is logically separated from the IAS to assure these levels of quality. The connection is characterised by an extensive use of traffic management in order to ensure adequate service characteristics and strict admission control.

Concepts such as a “logically separated” connection or strict admission control were abandoned in the final version of the Regulation based on an agreement of the co-legislators that technical definitions are not future proof and therefore limit innovation. This guideline disregards the intent of the legislation and provides an overly restrictive interpretation of the Regulation without legal basis and should therefore be deleted.

From a technical perspective in mobile networks it is useful to consider the workings of LTE QoS class identifiers where services can be assigned certain guaranteed throughput, VoLTE being an example. “Priority” is over radio, but only as far as to meet requirements, there is no general priority. The radio scheduler will use the parameters delay, loss ratio and guaranteed throughput as input only to assure the levels of quality. If strict admission control is used for a specific service (e.g. VoLTE) it will only be to protect other services that do not have these strict requirements. That is for instance, a

maximum bandwidth can be allocated a VoLTE service over a radio interface, and this is used for the strict admission control for VoLTE. This bandwidth will also be available for other traffic as far as it is not used by active VoLTE connections. With 5G, other ways of providing specialised services like network slices are available.

§107. NRAs should verify whether, and to what extent, optimised delivery is 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. To do this, the NRA should assess whether an electronic communication service, other than IAS, requires a level of quality that cannot be assured over an IAS. If not, these electronic communication services are likely to circumvent the provisions of the Regulation and are therefore not allowed.

This guideline suggests an authorisation process that is completely without legal basis in the Regulation. The Regulation is not about banning Services Other than IAS if they do not conform to certain requirements or conditions. On the contrary, providers of services, content and applications in the EU are guaranteed freedom to provide such services. The Regulation is about safeguarding Open Internet Access by striking down on practices that are undoubtedly harmful for the Open Internet.

The verifications and assessments performed by the NRA according to Article 3(5) have the objective to form the basis for interventions against services that either circumvent the Regulation – Article 3(5) first subparagraph - , or are offered as replacement for IAS or have detrimental effects on the availability or general quality of IAS – Article 3(5) second subparagraph.

If there is no suspected harm, there is no basis for intervention. As discussed elsewhere in this response, a polarized approach where everything is forbidden if it is not explicitly allowed is not justifiable. A strict “Two Lane Approach” has no legal basis in the Regulation. The principles of effectiveness, necessity and proportionality are central to all EU regulations and must be duly observed (see §177).

Within the field of 5G and IoT there are connectivity services that are neither IAS, nor do they fulfil some of the “requirements” for optimized services listed in the BEREC draft guidelines. If these “third category” connectivity services are to be forbidden based solely on definitions, then the guidelines will become a major hurdle for EU based 5G and IoT industry going forward.

For innovation to take place, the EU regulatory framework and its application at national level must be void of unwarranted restrictions. Any limitation in the freedom to provide innovative services must be predictable and objectively sensible. Needless to say such limitations must be based on clear and precise legal provisions adopted with due consideration of the impact of such legislation.

NRA interventions based on the Regulation should only be considered when market practices jeopardize the purpose of the Regulation, causing harm to end users or the functioning of the Internet. Interventions should then be effective, necessary and proportionate. It makes no sense to have restrictions based solely on definitions or requirements that are detached from their context, such as proposed in the BEREC guidelines. And it makes no sense that innovators should be dependent on NRAs for permission before investments in new and innovative services can be made. The guidelines must be amended to reflect the above considerations.

§108. The internet and the nature of IAS will evolve over time. A service that is deemed to be a specialised service today may not necessarily qualify as a specialised service in the future due to the fact that the optimisation of the service may not be required, as the general standard of IAS may have improved. On the other hand, additional services might emerge that need to be optimised, even as the standard of IAS improves. Given that we do not know what specialised services may emerge in the future, NRAs should assess whether a service qualifies as a specialised service on a case-by-case basis.

The case-by case approach is in line with the call for effectiveness, necessity and proportionality. As stated above there is no intrinsic value in NRAs performing assessments of all services in the market in order to qualify them in different categories (categories that may change over time). NRA assessments should instead take place only if there is reason to suspect that a certain service may be in direct breach of the provision regarding traffic management, are offered as replacement for IAS or are causing detriment to the availability or general quality of IAS.

§109. Typical examples of specialised services provided to end-users are VoLTE and linear broadcasting IPTV services with specific QoS requirements, subject to them meeting the requirements of the Regulation, in particular Article 3(5) first subparagraph. Under the same preconditions, other examples would include real-time health services (e.g. remote surgery) or “some services responding to a public interest or by some new machine-to-machine communications services” (Recital 16).

The “requirements” of the Regulation should not be about classifying optimized services into allowed ones and forbidden ones. They are instead intended to form the basis for NRA assessment leading to a decision to intervene against harmful practices alternatively to leave harmless practices alone.

When it comes to the list of “typical examples” of services that has an inherent need for optimized quality, BEREC states in §108 that such needs will likely change over time.

The list only contains three examples. As for the first, VoLTE, it should be mentioned that such calls can be delivered also over unmanaged wifi, i.e. without optimization of quality parameters.

§110. QoS might be especially important to corporate customers and these customers might be in need of specialised services which – as they are addressing businesses – are often referred to as “business services”. Such “business services” cover a wide array of services and have to be assessed on a case-by-case basis.

Please refer to comment to §108.

§111. Business customers often request services relating to virtual private networks (VPN), which are also discussed in paragraph 11 above. The term VPN can be used in relation to two different types of services:

- “VPN application”: A VPN application is typically used in the context of teleworking. A computer (e.g. an employee’s laptop) uses the public internet to connect to corporate services. In order to protect the information transferred, a VPN application on the client encrypts all traffic and typically

sends all traffic to a VPN concentrator located within the corporate network. Both ends - the client and the concentrator - use an IAS, and this would therefore not be a specialised service.

- “VPN network service”: A VPN network service is typically used to provide a private connection between a number of sites (e.g. different locations of a corporation). Such VPN services are typically implemented over common infrastructure with IAS (e.g. based on MPLS). Such services are provided in parallel with IAS. As long as the services comply with the requirements set out in the Regulation, they are considered to be specialised services.

For VPN network service the guideline states that such a service must comply with certain “requirements” in order to be considered to be optimized in the meaning of Article 3(5) first subparagraph. Among “requirements” listed by BEREC in §97 are that the optimization is objectively necessary in order to meet requirements for a specific level of quality.

However, the main driver for demand of VPN is not necessarily optimized levels of quality parameters such as speed, delay, jitter and packet loss. The business customer looks for a connection that is integrated in the company ICT architecture and is prioritized by the provider when it comes to issues like troubleshooting and restoring in the rare event of a network failure. It is not clear in the guideline that accommodation of such needs is considered by NRAs.

Further, by focusing on “VPN” the guideline illustrates its backward looking nature and its inability to cater for future developments. While one may make the distinction between a “VPN application” (over IAS) and “VPN network service” (over a specialised service), ISPs are moving towards SDN and NFV where dedicated private network resources will be replaced by software defined routers available in the Cloud and reachable on-line. By definition under SDN, “VPN network service” and “VPN application” will merge.

See also the comment under §11 and §123 regarding VPN.

Detailed comments to Article 3(5) second subparagraph

§112. Specialised services shall only be offered when the network capacity is sufficient such that the IAS is not degraded (e.g. due to increased latency or jitter or lack of bandwidth) by the addition of specialised services. Both in the short and in the long term, specialised services shall not lead to a deterioration of the general IAS quality for end-users. This can, for example, be achieved by additional investments in infrastructure which allow for additional capacity so that there is no negative impact on IAS quality.

It is not clear from the guidelines what reference points should be used when NRAs assess degradation/ deterioration of the availability and general quality of IAS.

Example: If a mobile network operator upgrades its mobile access network from LTE to LTE Advanced there will be a radical boost in speed and other quality parameters. If that operator after a couple of months implements a high definition live TV-service to all existing customers with premium subscriptions, there will likely be a significant impact on the IAS with typical download speeds decreasing from 150 Mbit/s to 100 Mbit/s in peak hours. 100 Mbit/s is still 5 times higher than the typical speed achievable before the upgrade. Has the general quality been degraded so much that the NRA should intervene? Must the operator invest in additional capacity so that the speed is restored at 150 Mbit/s in order to continue with its optimized service?

As the example above clearly shows, the concept of degradation/ deterioration is relative by nature and cannot be used without a case-by-case assessment of the facts in the matter. As for a reference

on how to assess the minimum baseline QoS of a IAS, the BEREC Guidelines BoR(12)131 could be applied.

It is common practice in some European fixed broadband markets that the ISP offers the basic connectivity and there is a choice for the end user between of a number of independent service providers, offering optimized service like IP-telephony and IP-TV. Since the Regulation is aimed both at ISPs and providers of content, applications and services, it is not always clear where NRA intervention will be targeted in the event of potential violations of Article 3(5) second subparagraph.

§113. In a network with limited capacity, IAS and specialised services could compete for overall network resources. In order to safeguard the availability of general quality of IAS, the Regulation does not allow specialised services if the network capacity is not sufficient to provide them in addition to any IAS provided, because this would lead to degradation of the IAS and thereby circumvent the Regulation. It is the general quality of the IAS which is protected from degradation by the Regulation, rather than specialised services.

It should be noted that limited capacity is not merely a vanishing problem as networks are constantly upgraded. Instead the explosion in data usage with exponential increase in the bandwidth that content and applications eat, there will continue to be limitations in network capacity even in the future. This holds especially true for mobile access networks. In fact there is no viable way to increase network capacity at the same rate as the ever increasing data usage. Mobile networks are dependent on traffic management in order to deliver the best possible user experience to the majority of users and this will not change going forward.

Furthermore, this draft guideline contains the same confusing conclusion as §107, i.e. that the degradation of IAS by an optimized service constitutes a circumvention of the Regulation (see the comment to §107).

§114. This implies that, in order to ensure the quality of specialised services, ISPs would have to ensure sufficient network capacity for both any IAS offers provided over the infrastructure and for specialised services. If not, provision of specialised services would not be allowed under the Regulation.

This guideline does not seem to be directed at NRAs, but rather sends a message to the ISPs. BEREC seems to have reversed the logic regarding the requirement not to degrade the general quality of IAS into something that appears as an obligation for ISPs to ensure a specific level of capacity. This is not the intention of the Regulation. Only when optimized services are provided in a way that degrades the availability or general quality of IAS should there be scope for NRA intervention.

Further, it is not clear how ISPs are supposed to prove that the capacity is sufficient. A reference to the BEREC Guidelines BoR (12) 131 would be appropriate here.

§115. NRAs could request information from ISPs regarding how sufficient capacity is ensured, and at which scale the service is offered (e.g. networks, coverage and end-users). NRAs could then assess how ISPs have estimated the additional capacity required for their specialised services and how they have ensured that network elements and connections have sufficient capacity available to provide specialised services in addition to any IAS provided.

NRAs should request information from ISPs regarding capacity only when there is an apparent problem relating to the Regulation. There is no merit in burdensome data collections, if there are no actual problems relating to the availability and general quality of IAS in the market.

It is unclear what questions ISPs could expect from NRAs when it comes to assessing sufficient capacity. What exactly are the network elements and connections referred to in the guideline? The term “connection” should not be understood to include IP-interconnect (see comments to §5-6)

§116. NRAs should assess whether or not there is sufficient capacity for IAS when specialised services are provided, for example, by performing measurements of IAS. Methodologies for such measurements have been relatively well developed during BEREC’s Net Neutrality QoS workstreams in recent years and will continue to be improved.

NRAs should not have to make assessments regarding network capacity if there are no recorded or anticipated problems in the market. The guideline should rather read; “NRAs *could* assess whether...”.

As for measurements it is our experience that third party applications for broadband speed tests are generally better than NRA developed.

§117. Specialised services are not permissible if they are to the detriment of the availability and general quality of the IAS. There is a correlation between the performance of the IAS offer (i.e. its availability and general quality) and whether there is sufficient capacity to provide specialised services in addition to IAS. IAS quality measurements could be performed with and without specialised services, both in the short term (measuring with specialised services on and off respectively) and in the long term (which would include measurements before the specialised services are introduced in the market as well as after). As Recital 17 clarifies, NRAs should “*assess the impact on the availability and general quality of IAS by analysing, inter alia, QoS parameters (such as latency, jitter and packet loss), the levels and effects of congestion in the network, actual versus advertised speeds and the performance of IAS as compared with services other than IAS*”.

As for the application of the “detriment” prerequisite, and its relation to the discussion of degradation /deterioration in §112, see the comment to §112 above.

It is not fully clear what BEREC means with the statement of correlation between IAS and the capacity to provide optimized services. Does BEREC mean that if the IAS performance is good then there is typically no detriment if optimized services are introduced?

As for the reference to Recital 17 it’s important to read the whole recital and not take selected parts and apply them out of context. NRA should analyse QoS parameters *if* there is suspicion of Services Other than IAS being used to the detriment of the availability or general quality of IAS. There is no merit in performing such analysis if there are no observed problems in the market.

§118. While IAS and specialised services directly compete for the dedicated part of an end-user’s capacity, the end-user himself may determine how to use it. Therefore, NRAs should not consider this an infringement of Article 3(5) second subparagraph, as long as the end-user is informed pursuant to Article 4(1)(c) of the likely or possible impact on his IAS and can still obtain a minimum speed for any IAS subscribed to in parallel. NRAs should not consider it to be to the detriment of the

general quality of IAS when activation of the specialised service by the individual end-user only affects his own IAS. However, detrimental effects should not occur in those parts of the network where capacity is shared between different end-users.

As for the understanding of what constitutes detrimental effects, see the comment to §112 above.

The reference to minimum speed should be clarified to mean the minimum speed as per the end-user's contract.

§119. Furthermore, as stated in Recital 17, in mobile networks - where the number of active users in a given cell, and consequently traffic volumes, are more difficult to anticipate than in fixed networks - the general quality of IAS for end-users should not be deemed to incur a detriment where the aggregate negative impact of specialised services is unavoidable, minimal and limited to a short duration. By contrast, such unforeseeable circumstances related to the number of users and traffic volumes do not normally occur in fixed networks.

This guideline does not give adequate guidance to the challenging statements in Recital 17 regarding negative impact in mobile networks. It deserves to be stressed that recitals are not binding legislation and it is not uncommon for courts to ignore statements in preambles and recitals that are ill-conceived. Further, the recitals should be read in their full context bearing in mind the purpose of the article it backs up, and not be referred to only in part and out of context. For a discussion on what constitutes detrimental effects, see the comment to §112 above.

It should be concluded in this guideline that the NRA assessment of negative impact in mobile networks should be made case-by-case and only if there is a recorded or anticipated problem that may call for intervention.

§120. NRAs should assess whether the provision of specialised services reduces general IAS quality by lowering measured download or upload speeds or, for example, by increasing delay, delay variation or packet loss. Normal small-scale temporal network fluctuation should not be considered to be to the detriment of the general quality. Network outages and other temporary problems caused by network faults, for example, should be treated separately.

As for the understanding of what constitutes detriment, see the comment to §112 above. When it comes to NRA assessments and measurements, it would be unnecessary to perform such mass surveillance if the NRA has no reason to suspect harmful practices in the market. The guideline should rather read; "NRAs could assess whether...".

§121. NRAs should intervene if persistent decreases in performance are detected for IAS. This could be detected if the measured performance is consistently above (for metrics such as latency, jitter or packet loss) or below (for metrics such as speed) a previously detected average level for a relatively long period of time such as hours or days), or if the difference between measurement results before and after the specialised service is introduced is statistically significant. In the case of short-term assessments, the difference between measurement results with and without the specialised service should be assessed similarly.

As for the understanding of what constitutes “persistent decreases in performance, see the comment regarding degradation/ deterioration §112 above.

Furthermore, NRA intervention should only occur if there is real harm, and measures should comply with due consideration of the principles of effectiveness, necessity and proportionality.

§122. It is of utmost importance that the provisions regarding specialised services do not serve as a potential circumvention of the Regulation. Therefore, NRAs should assess whether a specialised service is a potential substitute for the IAS, and if the capacity needed for their provision is to the detriment of the capacity available for IAS.

NRAs should not have to assess all optimized services in the market in order to fish for potential services that are in breach of the Regulation. Only when there is a problem in the market should the NRA take action.

The Article states that Services Other than IAS shall not be usable or offered as a replacement to IAS. In the recital this is elaborated by stating that the provisions in the Regulation should not be circumvented by means of such services usable or offered as replacement for IAS. However, in the guideline BEREC has distorted the message, now claiming the importance of the provisions not serving as a potential circumventing of the Regulation. This is followed by a conclusion that NRAs should assess if the service is a substitute to IAS and whether there is detriment for the available IAS capacity. This guideline is confusing and offers no guidance whatsoever to the NRAs. Instead the guideline should read; “If there is suspicion that Services Other than IAS are usable or offered as a replacement of IAS, the NRA should assess whether providing such services constitutes a circumvention of the Regulation. “

§123. In deciding whether a specialised service is considered as a replacement for an IAS, one important aspect that NRAs should assess is whether the service is actually providing access to the internet but in a restricted way, at a higher quality, or with differentiated traffic management. If so, this would be considered a circumvention of the Regulation.

This guideline is not in line with the Regulation as it makes presumptions regarding what constitutes a circumvention, that have no legal basis. In recital 17 it is concluded that a VPN service could offer access to the Internet and that this fact does not mean that such services are offered as replacements for IAS. If an optimized service, like a VPN service, offers restricted Internet access, at a higher quality or with differentiated traffic management this does not automatically disqualifies the service. Quite on the contrary could such a VPN service be absolutely legitimate in relation to its intended use, with no risk whatsoever to circumventing the Regulation. Further, from a technical perspective it is unclear what is meant by ‘higher quality’ and ‘differentiated traffic management’. This is too wide, and if the guidelines should have any meaning these two terms need to be specified.

This guideline is erroneous and must be amended or deleted.

Transparency measures

General comments

When issuing guidelines which govern transparency measures BEREC needs to observe the proportionality principle, being a general principle of Community law. Under this rule, the action of the Regulator must be limited to what is necessary to achieve the objectives of the Regulation. The undertaken measures must be reasonable, considering the competing interests of different groups at hand – industry and consumers. In our view there are certain guidelines which go beyond the purpose and need to be revised.

Detailed comments to Article 4(1) letter d

§126. NRAs should look to ensure that ISPs adhere to certain good practices regarding the information:

- it should be easily accessible and identifiable for what it is;
- it should be accurate and up to date;
- it should be meaningful to end-users, i.e. relevant, unambiguous and presented in a useful manner;
- it should not create an incorrect perception of the service provided to the end-user;
- it 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 the comparison can show differences and similarities.

We agree with the majority of this guideline. In particular we believe it is important that information provided in meaningful to end-users and no create any incorrect perceptions of the services provided. As we will discuss in our submission to other guidelines below BEREC has in some cases over reached in its suggestions for transparency with requirements that are sometimes impractical and in other cases may be misleading. We strongly urge BEREC to adhere to the many sensible principles as stated in §126. That said, we do have a concern with §126 related to information to be “...comparable between different offers, but preferably also between different ISPs ... in such way, that the comparison can show differences and similarities.”

Comparing services between different ISPs might not be possible since ISPs are not in the general fully aware of the functionalities, network and other technical conditions of another ISP and as such “show[ing] differences and similarities” may not be correct. In addition, even if the comparison was correct this may only be for a snap shot in time as technologies are constantly evolving. Further, such comparison may infringe competition regulations.

We suggest the requirements for provision of any comparison to different offers and ISPs go beyond the intention of the Regulations provisions and should be deleted.

§130. Articles 4(1), 4(2) and 4(3) apply to all contracts regardless of the date the contract is concluded or renewed. Article 4(4) applies only to contracts concluded or renewed from 29 November 2015.

§186. When monitoring and ensuring compliance with Articles 3 and 4, NRAs should take into account that the provisions of the Regulation apply to all existing and new contracts with the exception of Article 4(4), which applies only to contracts concluded or renewed from 29 November 2015. In turn, this means that, for a transitional period, Article 4(4) is not applicable to a certain amount of contracts. However, Article 4(4) will become applicable to more and more contracts over time once they are renewed or newly concluded.

The concept of legal certainty is recognized as one of the general principles of European Union law by the European Court of Justice since the 1960s. As a general principle in European Union law it means that the law must be certain, in that it is clear and precise, and its legal implications foreseeable. The doctrine of legitimate expectation, which has its roots in the principles of legal certainty and good faith, is also a central element of the general principle of legal certainty in European Union law. The principle of legitimate expectations, entails that a person is entitled to act (and to pursue his business enterprise) with the expectation that existing laws shall continue to apply. This means that a European Union institution, once it has induced a party to take a particular course of action, must not renege on its earlier position if doing so would cause the party to suffer loss.

Despite of the above mentioned principles, BEREC envisages in the draft guidelines that Articles 3 and 4 with the exception for Article 4(4) from the Regulation will apply to all existing contracts. In practice this means that IAS providers are obliged to change all existing contracts to apply the new measures. Beside the burdensome procedures for changing of the contracts with millions of customers, these changes will also trigger customer's rights under national laws, transposing the current regulatory framework for electronic communications networks and services, to withdraw from their contracts. This could cause unforeseen losses for the operators.

With regards to the transparency requirements set in Articles 4(1) – 4(3) it should be noted that only customers who concluded contracts after 29 November will have the right to trigger the remedies available to the consumer in accordance with the national law in case of non-conformity of performance of the internet access service. For contracts from before 29 November the amendment of the contracts to implement the Regulation would give the customers right to terminate their contracts without any reasonable grounds. Based on the above we urge BEREC to reconsider its position and to correct the Guidelines by preserving the general principles of European Union Law.

§137. In order to empower end-users, speed values required by the Article 4(1) letter (d) should be specified in the contract and published in such a manner that they can be verified and used to determine any discrepancy between the actual performance and what has been agreed in contract. Upload and download speeds should be provided as single numerical values in bits/second (e.g. kbit/s or Mbit/s). Speeds should be specified on the basis of the IP packet payload, and not based on a lower layer protocol.

§150. The estimated maximum speed for a mobile IAS should be specified so that the end-user can understand the realistically achievable maximum speed for their subscription in different locations in realistic usage conditions. The estimated maximum speed could be specified separately for different network technologies that affect the maximum speed available for an end-user. End-users should be able to understand that they may not be able to reach the maximum speed if their mobile terminal does not support the speed.

The Regulation obliges ISPs to specify “the estimated maximum and advertised download and upload speed of the internet access services in the case of mobile networks”. §137 refers to “actual

performance and what has been agreed in the contract” while §150 introduces a new expression that imposes significantly new and unpractical obligation on ISPs: “realistically achievable maximum speed... in different locations in realistic usage conditions”.

We believe that the draft guideline is too far reaching compared to the spirit of the Regulation. There is a large difference between the estimated maximum as stated in the Regulation and actual performance as stated in §137. A requirement to provide information for the “estimated maximum” speed as provided by the Regulation is achievable. The requirement to provide information on “actual performance” is going too far. For example, for mobile networks speeds can vary for several reasons, including:

- **Distance** from the base station, as well as any physical obstructions, such as walls, signal-blocking or reflecting materials affect signal propagation and reduce throughput. Actual performance could change also when a certain location changes over time, i.e. if a new building is constructed nearby, or
- **Interference**, which includes both self-interference (due to network load, as for example in the case of 3G networks) as well as external interference, or
- **Shared bandwidth** - The entire bandwidth available in a given cell is shared between all the users in the cell. In addition, some of the bandwidth is consumed by system signalling, the amount of which also depends on the load of the cell.

Any information on the actual performance at a certain place is valid solely and only for the very second it was measured. We believe the objective of better informing end users can be achieved by giving them an indication of the technology used and estimated maximum speed according to technology standards, coverage maps and factors that may influence the speed of the service. Thus, based on the information provided, end users are informed of the speed of the service they may expect in certain areas, at a certain time of the day/night, using a certain terminal.

We suggest that BEREC use the same wording as in the Regulation, namely “the estimated maximum and advertised download and upload speed”, which would mean theoretically achievable speed as far as this is measurable, precise and true.

§127. NRAs should ensure that ISPs include in the contract and publish the information referred to in Article 4(1) letters (a) to (e), preferably presented in two parts (levels of detail):

- The first part should provide high-level (general) information. The information about the IAS provided should include, for example, an explanation of speeds, examples of popular applications that can be used with a sufficient quality, and an explanation of how such applications are influenced by the limitations of the provided IAS. This part should include reference to the second part where the information required by Article 4(1) of the Regulation is provided in more detail.
- The second part would consist of more detailed technical parameters and their values and other relevant information defined in Article 4(1) of the Regulation and in these Guidelines.

§131. NRAs should ensure that ISPs include in the contract and publish a concise and comprehensive explanation of traffic management techniques applied in accordance with the second and third subparagraphs of Article 3(3), including the following information:

- how the measures might affect the end-user experience in general and with regard to specific applications (e.g. where specific categories of traffic are treated differently in accordance with Article 3). Practical examples should be used for this purpose;
- the circumstances and manner under which traffic management measures possibly having an impact as foreseen in Article 4(1) letter (a) are applied;
- any measures applied when managing traffic which uses personal data, the types of personal data used, and how ISPs ensure the privacy of end-users and protect their personal data when managing traffic.

§135. Regarding volume limitations, contracts should specify the ‘size’ of the cap (in quantitative terms), what that means in practice and the consequences of exceeding it (e.g. additional charges, speed restrictions, blocking of all traffic etc.). If the speed will decrease after a data cap has been reached, that should be taken into account when specifying speeds in a contract and publishing the information. Information and examples could also be provided about what kind of data usage would lead to a situation where the data cap is reached (e.g. indicative amount of time using popular applications, such as SD video, HD video and music streaming).

The draft guidelines above all reference the use of examples. The use of practical examples to end users, is indeed one of the ways of ensuring a comprehensible explanation on technical details, however, in terms of technology-based examples this could in some case be technically impossible or directly misleading. The draft guidelines above provide obligations on ISPs to:

- Split the information on General information and Detailed information (§ 127).
- Provide practical examples on how traffic management techniques might affect “the end-user experience in general and with regard to specific applications” (§ 131).
- Provide indicative amount of time using popular applications, such as SD video, HD video and music streaming which would lead to a situation where data cap is reached (§ 135).

First, these requirements go beyond the Regulation’s provisions, where only information on *how* related issues are going to affect end customers’ experience is set. Second, this kind of information is constantly changing due to the rapid rate of technological innovation.

Regarding data caps - specification of this information cannot be objective and relevant, since the time period during which data caps may be reached will depend on different circumstances, such as speed, topography, network configuration, weather, density, the number of users in the same locality. Most of these factors are far beyond the control of the ISPs. Further, data usage may vary even in the cases where similar type of data is being considered. As an example, video and audio files may use different encoding which can result in different file sizes for the same video/audio duration. In addition, applications and websites can include additional data (such as advertisements) while streaming, which would affect the data consumption of the user. Further, many applications use caching in order to improve the performance of audio/video streaming, which could result in more data being consumed even when the user terminates the streaming service before the end of the video/song. As such, it is not possible to accurately predict the amount of time in which the user will reach his data cap, even when using popular applications and services.

To the extent that BERC considers examples to be the most suitable way of achieving clarity for end users we believe should be published on the ISP websites, not in the contracts or General terms. This would also allow ISPs to change the examples as technology changes when it is considered necessary.

§152. Estimated maximum download and upload speeds could be made available in a geographical manner providing mobile IAS coverage maps with estimated/measured speed values of network coverage in all locations, including both indoor and outdoor coverage.

Provision of coverage maps to end users is one practical way of delivering information, but the requirement to show *“estimated/measured speed values of network coverage in all locations, including both indoor and outdoor coverage”* cannot be achieved.

There are many practical issues that arise from this draft guideline. First, there is no distinct method of measurement –when is the measurement taking place, who is responsible for defining all locations and where exactly is indoor to be measured (keeping in mind also, that “indoor” is mostly private properties, to which the ISPs do not have access). Second, should measurements be on an individual or average basis. Finally, it should be borne in mind that that the topography, surrounding buildings and a number of other factors may influence the speed provided at any point in time. Including these values would be extremely cumbersome for ISPs.