

Reply to public BEREC public consultation on the Net Neutrality Guidelines

Telia Company supports an open internet and values the EU's actions to safeguard it. We acknowledge that the task vested into BEREC in relation to the Regulation (EU) 2015/2120 (further - Regulation) is difficult, given the heated debate the topic has caused over the last few years and during the legislative process. We hereby present Telia Company recommendations on the most crucial aspects in the draft Guidelines (further - Guidelines).

Bigger picture

From more general point of view, with the current pace of innovation and upcoming launch of 5G, having both confidence in the regulatory environment and freedom to explore new commercial models is fundamental for European competitiveness in the digital eco system. We, as telecom operators, are not only being a conduit for others sectors, but more so we are primarily providing our customers with the services they demand at the quality they require.

Our view on the Guidelines

Telia Company believes that single most important aspect while drafting the Guidelines is to go back to the purpose of the legislation and to verify that each guideline serves the goal of open internet. These objectives, i.e. the equal and non-discriminatory treatment of the traffic as well as safeguarding related end-user rights, should be protected by the Guidelines. The current way the Regulation is being interpreted by BEREC raises concerns of potential creation of an 'innovation by permission' environment, as well as creating a barrier for efficient investment. While acknowledging the need for greater legal certainty when it comes to implementation of the Regulation, as a general remark we consider that Guidelines in a number of aspects go beyond its boundaries and BEREC's mandate. Therefore the Guidelines should be revised as listed in details below.

Legal assessment of BEREC's mandate

Regulation as a legal instrument is designed to ensure uniform application of EU law in all Member States. Regulation shall be sufficiently precise and unconditional with no discretion being left to the national authorities for implementation¹. Since the purpose of the regulation as the legal instrument is its direct effect into each Member State, no discretion is left for Member States.

¹ Article 288 of the Treaty of the Functioning of the European Union.

Therefore when it comes to BERECs mandate two questions shall be answered:

- 1) what are the general powers of BEREC under the Regulation EU 1211/2009² (further 2009 Regulation)
- 2) what are the limits of its powers in drafting the Guidelines

In general, BEREC's as an institutions mandate is described in the Regulation 121/2009. The mandate stipulates that NRAs shall take the utmost account of any guidelines issued by BEREC as long as those are issued in line with the powers described in Article 3(1) 2009 Regulation. Assuming that BEREC has powers to issue the Guidelines under 2009 Regulation (though it can also be disputed), the next question is what the limits of its mandate are when it comes to the content and subject matter of the Guidelines. Article 5(3) of the Regulation states that the purpose of BEREC when issuing the Guidelines is "to contribute to the consistent application of this Regulation" by "issuing the guidelines for the implementation of the obligations of NRAs". This means - no new rules on the substance of the Regulation can be developed by BEREC, rather focus on the implementation obligations of NRAs or in other words – the guidance by BEREC shall be limited to clarifying the implementation of the Regulation. Telia Company is of the opinion that in a number of guidelines (as will be listed below) this is not observed. In a number of cases the approach taken by BEREC results in detailed description which de facto creates new rules on the substance. In addition they are not covering all breadth of problems and sometimes are mainly illustrative – this could have been avoided if BEREC would in a restrictive manner recognized their task of the guidance.

Burden of proof

There are number of provisions in the guidelines which implies that the burden of proof lies with ISP's. However as an example, according to the Regulation recital 17, for Services other than Internet Access Services (SoIAS), that are allowed to be provided, it is the NRAs that shall demonstrate when a practice is in breach of the Regulation. Recital 17 of the regulation states "National regulatory authorities should verify whether and to what extent such optimisation is objectively necessary to ensure one or more specific and key features of the content [...]" In Guideline GL59 the burden has been shifted: IAS provider should justify that it is not violating the rules: "*In assessing whether a traffic management measure is reasonable, NRAs should assess the justification put forward by the ISP*". This goes against the general principles of law and reverses the burden of proof.

On the scope and subject matter of the Guidelines

No of GL in the Guidelines and the issue	Arguments	Proposal
GL4-5 Definition of end user to include CAPs –	BEREC incorrectly widens the definition of "end-user": namely the GL implies that both	GL4. According to the Framework Directive, "end-user" means a user not providing public communications networks or publicly available electronic

² Regulation (EC) No 1211/2009 of the European Parliament and the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office



<p>who is protected?</p>	<p>definitions - “user” and “end-user”³ - are part of the definition and should be taken into account and on that basis the rights of individuals, businesses, including consumers as well as CAPS are protected under the Guidelines. However the Regulation uses the term “end-users” and it is incorrect to widen its scope to also include CAPs. The way GL4 is formulated is a clear example of BEREC going beyond its mandate.</p>	<p>communications services. In turn, “user” means a legal entity or natural person using or requesting a publicly available electronic communications service. On that basis, BEREC understands “end-user” to encompass individuals and businesses, including consumers as well as CAPs.</p> <p>GL5. 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.</p>
<p>GL6 Interconnection</p>	<p>Issues like interconnection policies and practices of ISPs are not subject to the Regulation therefore they have no basis to be regulated by the Guidelines. These issues are subject to a different legislation stemming from the Access Directive (2002/19/EC).</p>	<p>GL6 to be deleted</p>
<p>GL17 Sub-internet service</p>	<p>The Regulation does not define the concept of “sub internet” while BEREC prohibits such type of offers. Authors of “soft law” (such as these Guidelines) are not vested with a right as the legislators and therefore Guidelines cannot come up with new definitions but should rather only interpret existing ones. Such practice (as “sub-internet” service) is portrayed as harmful and therefore illegal, but it is not foreseen in the Regulation. Yes, in can be harmful, but only after a case-by-case assessment based on the outlined rules of the Regulation</p> <p>From a practical point of view, the outright ban of such offers will obstruct the end-users interests because ISPs will not be able to offer such innovative services as eHealth or eGovernment SIM cards. It shall not be forgotten that innovation also happens in ISPs industry.</p>	<p>GL17 to be deleted</p>
<p>GL18 Applications where the</p>	<p>Such provision risks creating a discriminatory situation where limited access for “device-based” offers would be permitted, but</p>	<p>GL18. Services where the number of reachable end-points is limited by the nature of the terminal equipment used</p>

³ Art. 2 of Framework Directive (2002/21/EC) describes the definitions as : ‘end-user’ means a user not providing public communications networks or publicly available electronic communications services. ‘user’ means a legal entity or natural person using or requesting a publicly available electronic communications service;



<p>amount of reachable end-points is limited</p>	<p>application based are not. For instance an app installed on a smartphone (that app would have limited number of reachable end-points) would not be allowed. The principle of technological neutrality will be violated, which is safeguarded by the Regulation (Recital 2). Referring back to the aim of the Regulation - namely safeguarding end-users rights, such limitation as is demonstrated in GL18 would actually limit end-users right. Therefore when the customer demands such service where access to certain end points of the Internet will be limited, the terminal equipment shall not be the only mean where this functionality can be implemented.</p>	<p>with such services (e.g. services designed for communication with BoR (16) 94 7 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</p>
--	---	---

Commercial practices

Ex post assessment. It is undisputable based on the wording of the Regulation that NRAs monitoring obligation is only meant to be ex post, being on commercial offers or SoIAS, however the Guidelines goes beyond this. The way the Guidelines are currently drafted create uncertainty in the respect about *ex post* versus *ex ante* and therefore should be modified. In our opinion, if the Guidelines will be approved in its current form, they will result in unintended consequences which will have negative outcomes for consumers whose rights will rather be limited and the outcome will also be stifled innovation and lack of choice. We therefore call for a deeper reliance on well-established EU competition law and case-law rather than invention of the new rules and criteria's for assessment as currently outlined in the Guidelines. In addition, the Regulation is not a law designed to regulate general commercial partnerships, marketing, pricing and product issues. As rightly acknowledged by BEREC in GL42, different types of zero-rated practices can have different effects on end-users. Therefore effect based approach shall be clearly reiterated in evaluating commercial practices on case-by-case basis.

No of GL in the Guidelines and the issue	Arguments	Proposal
<p>GL25 Prohibition to restrict tethering</p>	<p>Restricting tethering is seen as restriction of end-users' choice of terminal equipment – namely it is claimed to likely constitute “a restriction on the use of terminal equipment <u>connecting to the network</u>”. On the one hand, ISP restricting tethering in agreements, does not restrict equipment connected to the network, because when the customer is tethering only one piece of terminal equipment is connected to the network all other devices are</p>	<p>GL25. 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</p>



	<p>connected to this original terminal. Hence those other devices cannot be considered as “<i>terminal equipment connected to the network</i>” (see definition of “terminal equipment” in the Directive 2008/63/EC). On the other hand, not allowing for operators to restrict tethering will impede the ISPs willingness to create and promote unlimited data offers, because end-users could then use their one portable devices as Wi-Fi hot spots or link their smart TV to their mobile phone to stream in an unlimited manner. Besides legal arguments, it should also be assessed on the larger scale what benefits such a general “non-restriction “ would provide for the end-users and what it would deprive them off.</p>	<p>tethering 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).</p>
<p>GL38 and GL45 Ban of zero-rating of one application</p>	<p>An outright ban of the zero rated offers (GL 38) or negative stand towards them (GL 45) in the Guidelines contradicts the Regulation to the extent that BEREC goes beyond the legal ground. Case-by-case assessment should be the assessment method, not a single de facto description of what is declared illegal under the Regulation. See comments on BEREC mandate above and more arguments under the comments for GL42 and GL52.</p> <p>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 try new services or to use them for customer service (topping-up the mobile data bucket when the initial amount will be consumed) or speed test without having to worry about data consumption costs.</p>	<p>GL38, GL45 to be deleted in their entirety</p>
<p>GL39 Zero-rating of entire category as opposed to one application</p>	<p>Such fragmented and one sided theoretical analysis made beforehand with the conclusion that it “<i>creates an economic incentive to use that music applications instead of competing ones</i>” is flawed. The aim of the Regulation is not to limit commercial offers and as outlined in the beginning of this paper - BEREC has no mandate to formulate new laws nor issue an assumptions in advance of what is legal and what is not without case-by-case assessment.</p>	<p>GL39. 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</p>



		<p>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.</p>
GL42 Lack of test for assessment	<p>Recital 7 of the Regulation states that NRAs should be empowered to intervene against agreements or commercial practices which, by reason of their scale, lead to situations where end-users’ choice is materially reduced in practice. In our opinion, it is clear that the legislator has focused on an ex post case by case assessment, based on the following criteria for commercial practices:</p> <ol style="list-style-type: none"> <u>Scale</u> of the practice <u>Materiality</u> in reduction of end-user’s choice Reduction of the choice <u>in practice</u> 	<p>Addition to GL42 to be inserted: <i>“The following test for assessment of the questioned commercial practice shall be carried out and all 3 aspects to be assessed:</i></p> <ol style="list-style-type: none"> <i>Scale of the practice</i> <i>Materiality in reduction of end-user’s choice</i> <i>Reduction of the choice in practice</i> <p><i>This assessment shall be carried out in line with the well-established EU competition law methods and principles”</i></p>
GL43 Impact on Freedom of expression	<p>The last bullet in GL43 states that one of the aspects to assess when it comes to commercial practices and their impact on end-users choice is the effect they will have on the freedom of expression and media pluralism. The Guidelines also gives reference to Recital 13. Firstly, Recital 13 is concerning traffic management going beyond what is considered reasonable (first exception) and to refer to it in the context of the commercial practices is erroneous . Secondly, the Regulation does not address the issues of media and freedom of expression neither vests the NRAs or other competent authority the obligation to observe it in “open internet” context. There are other laws dealing with these issues.</p>	<p>GL 43 The last bullet point to be deleted:</p> <ul style="list-style-type: none"> the effect on freedom of expression and media pluralism (ref. Recital 13).
GL52 Technical discrimination	<p>Zero-rated offers where all applications are blocked (slowed down) once the data cap is exceeded except for the zero-rated application are considered technical blocking and against traffic management provisions because of the discrimination of the traffic. <u>Firstly</u>, as mentioned above, a prior prohibition of commercial practice goes beyond BEREC’s mandate. <u>Secondly</u>, it is important to go back and identify what non-discrimination principle means in the context of EU law. Non-discrimination is a general principle of EU law and therefore has higher norm than the one referred to in the Regulation. The concept of discrimination under the Guidelines appears to be broader and vaguer than the corresponding concept under EU law. In</p>	<p>GL 52 (Third bullet to be deleted)</p> <ul style="list-style-type: none"> 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), as it would infringe Article 3(3) first (and third) subparagraph.



	<p>principle, when assessing the cases of discrimination, the assessment should be limited to whether the measure constitutes a disadvantage and, if so, whether the measure is objectively justified. This is widely used approach in EU Competition law, and BEREC shall follow the well-established rules. For a disadvantage stemming from discrimination to be acknowledged under EU law and settled case law, it requires that damage or harm is shown. Building on this premise it is important that the Guidelines outline that every commercial practice or traffic management measure before being declared to infringe the Regulation on the basis of discrimination, firstly undergoes the above described assessment.</p> <p><u>Thirdly</u>, evaluating this from purely legal perspective, the Regulation (Article 3.2 and the preamble paragraph 7) allows for agreements to be entered into with different tariffs related to a certain amounts of data. The measure to be taken as to hindering further usage of data once the commercially agreed cap is reached, aims to uphold the subscriber contract. This action cannot reasonably be considered to limit the end user's rights under Article 3.1.</p> <p>Imposition of the data cap is based on the voluntary contracts with the subscriber which are allowed under the Regulation. The question then is on what basis ISP by default (without carrying out a discrimination assessment) also should block the zero rated content? There is no contractual or other commercial ground to hinder the "zero rated" content. The purpose of the zero rated offer is that this traffic is unlimited. There is therefore no reason to hinder the zero rated traffic just because the subscriber has exhausted its pay-traffic and not paying for more. It would be an unjustified and an unnecessary intrusive measure against the end-user.</p>	
--	---	--

Traffic management

In the onset of 5G, new interpretations by BEREC towards how capacity can and should be managed efficiently risk overregulation. Given the particularities of the electronic communications industry and how interlinked it is with technology advancements, regulatory approach in the Telecoms Framework⁴ established that ex ante regulation shall be forward looking, so that it shall not hamper innovation. BEREC guidelines should not prevent or obstruct the emergence of network evolutions based on 5G or SDN/NFV solutions.

⁴ DIRECTIVE 2002/21/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)



As acknowledged by the Regulation, reasonable traffic management is necessary and should not be opposed to investment that remains operators' decision. It is simply wrong to consider 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).

No of GL in the Guidelines and the issue	Arguments	Proposal
GL50 Packets treated agnostically	Traffic today and even more so in a 5G world will have different needs and cannot be processed in a way that is <i>“agnostic to sender and receiver, to the content accessed or distributed, and to the application or service used or provided”</i> .	GL50 to be deleted
GL51 Network internal assisted end-point congestion control and agnostic treatment	“Application agnostic” is not realistic due to the varying scenarios defined by end-point capabilities and location.	GL 51.Endpoint-based congestion control (a typical example is Transmission Control Protocol (TCP) congestion control) does not contravene Article 3(3) first subparagraph since, by definition, it takes place within terminal equipment and terminal equipment is not covered by the Regulation. ¹² NRAs should consider network-internal mechanisms of ISPs which assist endpoint-based congestion control ¹³ to be in line with equal treatment, and therefore permissible, as long as these mechanisms are agnostic to the applications running in the endpoints and a circumvention of the Regulation does not take place.
GL60 Explanation of the categories of traffic	It is stated that traffic categories should typically be defined based on QoS requirements whereby a traffic category will contain a flow of packets from applications with equal requirements. Therefore, if ISPs implement different technical QoS requirements of specific categories of traffic, this should be done objectively <u>by basing them on the characteristics of the applications transmitting the packets</u> . We would like to note that quantifying the QoS requirements by basing them only on the characteristics of the applications transmitting the packets is not sufficient. In addition, the use cases have a major significance that must be taken into account. For example the “criticality factor” should be considered as for example blue light services (not just voice) or various industry segments (health care, banking, manufacturing processes, etc.) using similar type of applications in different use cases/scenarios. The Regulation states that in order to be reasonable, traffic management measures shall be based on objectively different <u>technical quality of service requirements</u> of specific categories of	60.Traffic categories should typically be defined based on QoS requirements, whereby a traffic category will contain a flow of packets from applications with equal (similar) requirements. Therefore, if ISPs implement different technical QoS requirements of specific categories of traffic, this should be done objectively by basing them on the <u>criticality factor and</u> characteristics of the applications transmitting the packets. For example, such a category may consist of real-time applications requiring a short time delay between sender and receiver.



	traffic". We believe that "criticality" is related to technical quality of service requirements.	
GL61 ISP to rely on the information provided in the packet. Encryption	The Guidelines imply that, in order to decide whether or not to apply network management measures on a certain packet, IAS providers should rely on information provided by either the header of the packets itself or directly by the content provider when the traffic is encrypted and the IAS provider has no means to verify the kind of traffic it is transporting. This would lead to a high degree of risk for the IAS provider, opening the door to fraud, either by mismatching the header with the real content or by declaring one traffic for another in case of encryption. In some cases, when the application uses proprietary protocols, it would even be impossible from a technical point of view. To obligate ISPs to manage traffic on the above described basis would be unjustified and would entail the risk for normal functioning of internet.	GL61. 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.
GL54 Traffic management as <i>prima facie</i> infringing the principles or reasonable traffic management	There is no legal basis to reverse assumption of traffic management, that by default it is unreasonable if not proven otherwise. BEREC guidelines should therefore not include wording such as " <i>prima facie appears to infringe this principles</i> ". NRAs should be concerned by the outcomes of traffic management, not by monitoring the technical options chosen by each ISP to achieve these outcomes.	GL54. 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.
GL66, GL67 Not monitoring specific content (i.e. transport layer protocol payload)	The Guidelines explain further what are the boundaries when it comes to not monitoring the specific content in the course of reasonable traffic management: namely only information contained in the IP header and the TCP may be used. However, such information is not very indicative. Traffic Monitoring must also be allowed for Traffic Detection Functionality for the purpose of correctly applying traffic management policies for flows and aggregates of traffic in line with the Regulation goals. In addition, defining content as payload of transport layer is too restrictive - also protocols within e.g. TCP and UDP can be of generic type (e.g. Web-RTC and SIP protocols).	GL 66. In assessing traffic management measures, NRAs should ensure that such measures do not monitor the specific content. (i.e. transport layer protocol payload). GL 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).



<p>GL 88 Congestion control based on Comcast model</p>	<p>We believe it is not correct to argue for agnostic feasibility based on the COMCAST model defined in the <u>informational</u> RFC6057 – it is a highly limited use case restricted to a peripheral network segment designed with almost completely for IAS (as referenced by the RFC itself as "Comcast Internet Backbone") rather than a multiservice backbone network service for almost all conceivable traffic types and use cases of telecommunication. In our opinion, the solution is highly dependent on sender/receiver information, i.e. monitoring a customer specific port.</p>	<p>GL 88 Congestion management can be done on a general basis, independent of applications. NRAs should consider whether such types of congestion management would be sufficient and equally effective to manage congestion, in light of the principle of proportionality. For the same reason, NRAs should consider whether <i>throttling</i> of traffic, as opposed to <i>blocking</i> of traffic, would be sufficient and equally effective to manage congestion.</p>
<p>GL 89 NRAs to monitor dimensioning of the networks. Congestion control</p>	<p>This is another example where the draft Guidelines are more restrictive than the Regulation – the Guidelines states that NRAs are required to monitor that ISPs <i>properly dimension their network</i> and application-specific congestion management should not be applied or accepted as a substitute for more structural solutions, such as expansion of network capacity (89). The Regulation does not provide for such an intrusive and far reaching right of the NRA to oversee the dimensioning of the networks by the operators.</p> <p>Firstly, this requirement is not necessary since it is natural that ISP's in a competitive market will strive to ensure sufficient capacity to meet his customers' requirements for QoS. Secondly, this entails that NRA's will have to be involved in daily operations of the ISP's which is neither proportionate nor has a legal basis.</p> <p>When it comes to congestion control, the whole internet ecosystem shall be taken into account and therefore IAS liability will be limited. For instance CAPs can operate their own networks and it will depend on the dimensioning of their access to internet or their interconnection. ISP cannot be liable for congestion which occurs outside of our control.</p> <p>Another aspect is a resent trend resulting from increasingly higher access speeds in comparison to backbone speeds that has introduced challenges in form of extreme and unpredictable traffic bursts from single sources. This is an effect of end points trying to maximize throughput without reasonable quality requirements, causing recurring random short term congestion events, which is becoming a state of normality. This phenomena should be taken into consideration so that ISPs can effectively mitigate it by burst control (policing/shaping) for the benefit of transmission quality optimization.</p>	<p>NRAs should monitor that ISPs properly dimension their network, and take into account the following:</p> <ul style="list-style-type: none"> □ 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); □ application specific congestion management should not be applied or accepted as a substitute for more structural solutions, such as expansion of network capacity.



<p>GL111 example</p> <p>VPN</p>	<p>From a legal point of view, the Regulation does not differentiate VPN services by technology. Recital 17 states <i>“the mere fact that corporate services such as virtual private networks might also give access to the internet should not result in them being considered to be replacement of internet access services...”</i></p> <p>From technical point of view, the location of a VPN access (ingress) point should not limit the customer use cases, application and specifically not the quality requirements:</p> <ul style="list-style-type: none"> (i) A VPN initiating in the customer end/premises should not have any bearing on whether the service constitutes a "specialized service". Supporting customer QoS requirements usually initiates in the customer-premises equipment (CPE) where the customer has the right to implement any local QoS functionality. Often however, this design and implementation is offered to the customer as a Value Added Service. With this limitation in the Guidelines this VAS would not be possible to provide and would not be in the benefit of the customer. (ii) Also in the case of network based VPN the access point of quality differentiation starts at the customer end (CPE/Terminal). <p>In addition, the division between “VPN application” (over IAS) and “VPN network service” (as SoIAS) is not future proof, primarily because of developments in SDN and NFV. In the future architectures, existing dedicated private networks will be replaced by software defined routers available in the Cloud and reachable on-line. As such, “VPN network service” and “VPN application” will become one.</p>	<p>GL111 to be deleted</p>
<p>GL75 Prohibition of network level ad blocking (and spam/parental controls)</p>	<p>The Guidelines gives an example that advertising blocking: if chosen by end user (terminal equipment-based) is permitted. However if the blocking would be network-based it would not be allowed if the exception for reasonable traffic management is not met. This is potentially discriminatory and not technologically neutral (network level vs terminal equipment based) – in essence the outcome shall be important (“open internet”), but not on which level it is technically executed</p>	<p>GL75. By way of example, ISPs should not block, slow down, alter, restrict, interfere with, degrade or discriminate advertising when providing an IAS, unless the conditions of the exceptions a), b) or c) are met in a specific case. In contrast to <i>In such case, as long as there is end-users will under the contract, network-internal blocking put in place by the ISP and terminal equipment-based restrictions put in place by the end-user shall be allowed and both means treated equally.</i></p>



GL95 “Standard best effort delivery”	Referring to "standard best effort delivery" is highly questionable since there is no "standard" quality defined for best effort. Instead “general IAS quality” would be more applicable.	GL95. 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 <u>general IAS quality</u> .

Services other than IAS

When it comes to SoIAS, the focus of the Guidelines seems to be to put ISP's in a disadvantageous position compared to other service/content providers by restricting their freedom to innovate. It is of the utmost importance to acknowledge that the innovation in the ICT sector also is carried out by the ISP industry and the Regulation was not aimed at restricting this. There should be a balance between freedom to provide SoIAS and forcing for the structural remedies (requirements) to invest.

There is no non-discrimination requirement in the Regulation between IAS traffic and SoIAS: the aim is to guarantee that services with higher quality needs can also be delivered over IAS. When it comes to monitoring of SoIAS, it should be done ex post according to the Regulation.

The needs of business customers shall be addressed properly. This is an important issue, because operators have business customers with critical needs for their communications. Due to unsatisfactory BEREC treatment of VPN, there is a risk that operators cannot meet the demand for business critical services.

No of GL in the Guidelines and the issue	Arguments	Proposal
GL101, 104 Optimization of SoIAS	<p>(101) While the Regulation grants NRAs the power to verify whether the optimisation is necessary, it shall not lead to “innovation by permission” environment and BEREC should apply <i>ex post</i> regime to verify if the service is delivered in line with the requirements.</p> <p>(104)The paragraph misinterprets the Regulation when it comes to the freedom to provide SoIAS. Namely the GL implies that there is a burden of proof on the provider of SoIAS to demonstrate the necessity of optimization for SoIAS <u>independently of their impact on IAS</u>. The “independently of their impact on IAS” requirement is unclear, because of the following:</p>	<p>GL 101. NRAs should “<i>verify</i>” 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.</p> <p>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</p>



	<p>(i) the idea of SolIAS is addressed by the Regulation because of their relation and possible impact on the IAS.</p> <p>(ii) SolIAS are neither defined nor regulated by the Regulation except for the case when it is used to circumvent the obligations put forward on IAS.</p> <p>(iii) NRAs power to investigate the optimization of SolIAS independently of IAS is going beyond the aim of the Regulation.</p>	<p>requirements are (e.g. latency, jitter and packet loss), and any contractual requirements. Furthermore, the “<i>specific level of quality</i>” should be specified, and it should be demonstrated that this specific level of quality cannot be assured over the IAS. These provisions do not imply “authorisation” regime by NRAs for SolIAS.</p>
GL106 SolIAS offered through logically separate connection	<p>BEREC assumes that SolIAS are always offered via separate connection, however it can be provided in a few ways – separately or in combination with IAS. Therefore the requirement in the Guidelines that SolIAS are offered only via logically separate connection are superfluous and ungrounded compared with the Regulation.</p> <p>It is also unclear what is meant by "strict admission control". Admission control for individual applications, end users or terminals would be unnecessarily strict and complicated to implement. Particularly so for typical business customers with a broad range of applications and changing environment. Instead, admission control according to agreed Service Level Specification defining the traffic profile and classification criteria should be sufficient.</p>	<p>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 <i>agreed in Service Level Specification defining the traffic profile and classification.</i></p>
GL117 Measurements	<p>Turning SolIAS off during measurements is impossible, it can simply not be done since this will obstruct customer experience and trigger liability on the service providers side – the customers expect continuous availability of SolIAS.</p> <p>The other aspect of this paragraph implies prior “authorisation” by NRAs before SolIAS are introduced to market and therefore shall be deleted.</p>	<p>GL 117[...]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)[...]</p>

Transparency measures

It is important to notice yet again that the Regulation clearly limits BEREC’s mandate – namely it states that BEREC shall issue the guidelines for the implementation of the obligations of NRA under Art. 5 “Supervision and enforcement”. In many Member States there are number of industry and regulatory solutions already in place to address the marketing of speeds which are generally a result of extensive discussions and consultation processes that reflect the particularities and factors of each country. These policies are widely accepted and used in practice. The aim of the guidelines was not to come up with the unified approach to marketing of internet speeds in EU, since it would undermine the principle of subsidiarity and existing legislation. The purpose of the Guidelines when it comes to transparency obligation should be to provide guidance on how customers should receive “*clear and comprehensive explanation of minimum, normally available and maximum speeds*”. However, the current Guidelines on Art. 4 of the Regulation is far reaching and very prescriptive and there are too many detailed requirements on the information to



the end-users (GL124-163) which are disproportionate. In essence under Art. 4 the Regulation foresees a technical function which shall be satisfied by proportionate regulatory burden on ISPs with sufficient legal certainty.

No of GL in the Guidelines and the issue	Arguments	Proposal
GL130 retroactive application of conditions (to both new and existing contracts)	BEREC guidelines state that Art. 4(1)-4(3) shall be applicable to all contracts regardless of the date the contract is concluded or renewed. Legal certainty is a well established general principle of EU law. It means that legal implications of the legislation shall be foreseeable ⁵ . Furthermore, ECJ established that the principle of non-retroactivity and principle of legitimate expectations lies within the general principal of legal certainty ⁶ . There are exceptions under which retroactivity shall be applied, namely in <i>GrSa Fleisch</i> case, the ECJ stated that the substantive rules of Community law must be interpreted as applying to situations existing before their entry into force <u>only in so far as it clearly follows from their terms, objectives or general scheme that such effect must be given to them</u> ⁷ . Therefore since the Regulation does not state that Art. 4(1)-4(3) shall enter into force from a different date than the whole Regulation, such interpretation of GL130 shall be considered illegal. If legislators would have had an aim to have these rules apply retroactivity, it would have used the wording as in Art. 4(4) which explicitly stated the earlier date of entry into force of that provision.	GL130. 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.
GL126 ISPs to adhere to good practices	There is no basis in the Regulation to impose on ISPs best practices regarding the information, especially comparability of offers.	GL126 to be deleted as each country has its own best practice based on the local circumstances (networks, technologies, geography)
GL127 Level of detail for information	Guidelines yet again goes further into details than outlined in the Regulation, by requiring to present the information in two parts: general and detailed. Namely under the detailed part ISP will have to publish " <i>more detailed technical parameters</i> ". Such requirements are ungrounded since already under the current Regulatory framework including Universal Service Directive ⁸ and Consumers Rights Directive ⁹ ISPs are providing a lot of specific information to end-users.	GL127 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 it 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

⁵ Case 325/85 *Ireland v Commission* [1987] ECR 5041

⁶ For example, in the case 234/83 *Gesamthochschule Duisburg v Hauptzollamt Munchen – Mitte* [1985] ECR 327

⁸ Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002

⁹ Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011



		<p>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.</p> <p><input type="checkbox"/> 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.</p>
<p>GL137-154 Detailed technical parameters on speeds</p>	<p>BEREC goes beyond the Regulation when it comes to implementation of the Art. 4 (1)(d) on “<i>Clear and comprehensive explanation of the minimum, normally available, maximum and advertised speeds...</i>” because it takes a very detailed approach and turns explanations on speed into the detailed technical parameters to be foreseen in individual contracts. “<i>Clear and comprehensive</i>” translates into “<i>specific</i> (sometimes even numerical) <i>technical parameters</i>”.</p> <p>For example, in GL141 BEREC’s far reaching and prescriptive recommendation on speed ranges with regard to Art. 4 (1) letter (d) are impractical. For technical reasons, ISPs cannot contractually agree a single speed parameter but have to agree speed ranges. A possibly strict limitation of maximum speed by NRAs such as recommended in BEREC’s proportionality criteria in GL 141 risks that that de-facto providers will only indicate lower maximum speed in the contract. This may apply even if the available speed for customers is much higher. Customers would not be informed any more about the realistically available maximum speed. This will also directly impact advertised maximum speed, which, according to BEREC, must not be higher than the contractual maximum speed.</p> <p>Or another example of GL142 - BEREC recommends that the maximum speed of fixed IAS indicated in the contract has to be achieved by the end-user at least some of the time and gives an example of “<u>once a day</u>”.</p> <p>In addition, while published information is per se general and non-individual, BEREC recommends the provisioning of customised technical parameters <u>in individual contracts</u> (e.g. individual speed ranges). The publication of customised contractual information are of no value for end-users who want to compare different offerings and ISPs would be required to publish a huge variety of different information. BEREC should clarify that publication of information has to refer to general information. Also, assuming they fall within the scope of an IAS, individually agreed contracts cannot reasonably include customised technical parameters and should not require publication.</p>	<p>To delete detailed provisions from GL137-154.</p> <p>Instead of going beyond Regulation and restricting maximum and advertised speeds, BEREC should only recommend a reasonable definition of “<i>normally available speed</i>” without numerical value which matches with the experience of most customers.</p>

