BEREC Public Consultation

"On the implementation by National Regulators of European Net Neutrality rules"

(Consultation reference: BoR (16) 94)

Contribution from PT Portugal

I. Introduction

PT Portugal welcomes the opportunity given by BEREC to comment the guidelines for the implementation, by National Regulators, of the European Net Neutrality rules.

We believe, however, that the process followed and its results (until now) put at risk the development of efficient and technological advanced services, which require a future-proof, flexible and coherent regulatory framework, contrary to what we fear may result from a wrongful interpretation and implementation of the European Regulation 2015/2120 of 25 November 2015 (hereinafter the TSM Regulation). In fact, prior and further interactions between BEREC and the industry while the draft guidelines were being developed would have prevented some of the issues that we shall discuss next.

We would like to emphasize the fact that Net Neutrality has never been a real problem in most of the EU Member States, and especially in Portugal, which is mainly due to the existence of a competitive IAS market, allied to and promoted by a regulatory framework that ensures transparency, enabling customers to make informed decisions.

Therefore, we are very concerned that BEREC's guidelines may become excessively detailed and restrictive, creating, in our view, risks of various kinds: technological inadequacy, disregard for fundamental principles of the regulatory framework (necessity, appropriateness, proportionality) and extension of the provisions contained in the TSM Regulation.

We thus urge BEREC to pursue a path whereby the interpretation and implementation of TSM Regulation is properly weighted and does not result in the imposition of burdens and restrictions other than necessary, justified or proportionate.

We advocate, for such, that it is necessary to preserve the proper flexibility for NRAs to suit the implementation of the TSM Regulation to their national circumstances. This requires the guidelines to be based on general principles which give sufficient latitude for NRA, instead of seeking to establish closed and restrictive interpretations, limited in scope, quickly becoming

obsolete and even contrary to the Regulation in what concerns the protection of end-users' choices. [1]

We therefore consider that the draft guidelines should be reviewed on several key aspects as they go beyond what is necessary to implement the Regulation and/or risk hampering innovation with a too static interpretation of networks' evolution and markets' functioning. Our main concerns are detailed below and address:

- scope of the guidelines and its definitions
- open internet access and commercial practices
- traffic management
- services other than IAS (SoIAS)
- QoS measures, transparency and monitoring system's certification
- supervision and enforcement.

II. Detailed comments

1. **Scope and definitions** (referring to Articles 1 and 2)

a) Scope:

We consider that the draft guidelines go beyond the mandate given to BEREC by the TSM Regulation, namely to "issue guidelines for the implementation of the obligations of national regulatory authorities" and the scope of the Regulation itself ("laying down measures concerning open internet access" and establishing "common rules [...] in the provision of internet access services").

In fact, the guidelines should focus on just ensuring an open Internet access, and not on services other than IAS or the made up "sub internet services" concept (which isn't even

[1] PT Portugal recalls the decisive position that BEREC took in October, 2013 on the TSM Regulation proposed by the European Commission. At the time, BEREC said that best practices are identified by a bottom-up process when an NRA innovates and tries something different, which is shown to work and then goes on to be adopted by other NRAs. We totally agree with this principle and we expect to see it respected also in what concerns the Net Neutrality Guidelines.

mentioned in the Regulation), and should aim to give harmonized guidance to NRAs and not to prescribe prohibitions for the operators.

b) CAPs as end-users:

BEREC does not properly explain the rationale for the inclusion of individuals, business companies as well as CAP (Content and Application Providers) in the definition of "end-user".

Considering the definition of end-user as an entity that does not provide public ECS (electronic communication services) the inclusion of CAP in the concept of end-user is yet another reflexion of the lack of level playing field between ECS providers and OTT. Since this Level Playing Field is expected to be set in the forthcoming Framework Review (at least in what concerns OTT-0 and OTT-1, using BEREC's taxonomy), this guideline does not seem future proof as many CAP will not respect the definition of end-user.

Furthermore, it is clear that CAP's nature is not compliant with an "end-user" concept in the spirit of TSM, and BEREC's guideline, in considering the opposite, largely exceeds the scope of the Framework Directive and the TSM regulation.

In fact, CAPs may comprise, for instance, and according to our interpretation of BEREC's definition:

- a person/individual who provides a public blog/webpage
- an online edition of a newspaper (e.g. The Wall Street Journal)
- a TV channel multicasting over an IPTV broadband access (e.g. Fox News)
- a search engine company (e.g Google)
- an OTT providing communication services (e.g. Skype)
- a social network provider (e.g. Facebook).

But the nature of the TSM Regulation is to protect end-users' rights on the retail market and BEREC's definition enables misunderstandings and confusion.

On the other hand, interconnection issues, including between CAP and ISPs, are out of the scope of the TSM Regulation.

Thus, paragraph 4 of the draft guidelines needs to be reviewed accordingly and paragraphs 5 and 6 should be withdrawn.

c) Customers and end-users

To include "business end-users" and "consumer end-users" in a larger broad definition of end-users creates legal uncertainties and unjustifiable restrictions.

In fact, the access of business end-users to services depends mostly on the business subscribers' choices and conditions (Cf. 2002/21/CE Framework Directive "Article 2, Definitions, (k) subscriber: means any natural person or legal entity who or which is party to a contract with the provider of publicly available electronic communications services for the supply of such services). And the "business subscriber" also has rights, one of which is to define the rules for ECS (and IAS) usage and access applicable to its employees (the end-users). E.g., a company ("business subscriber") may define that all or part of its own employees ("business users") may not access the international voice network at all (due to costs, department functions or any other business criteria to maximize productivity). The same applies to IAS.

And furthermore, a user ("subscriber") should be allowed to contract any kind of IAS that serves its requirements and even to request blockage of certain categories of traffic and/or protocols. Accordingly, paragraphs 17, 35 and 52 of the draft guidelines should be deleted.

d) The Nature of a VPN from a subscriber point of view

In our view a VPN may be:

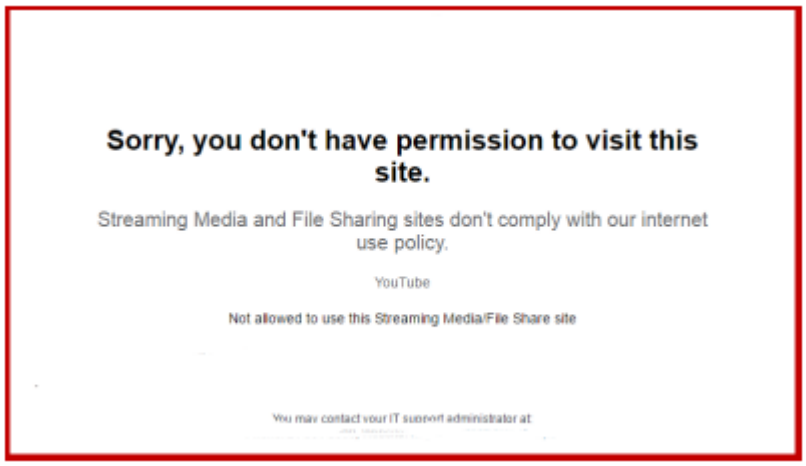
- A (subscribed) encrypted service that enables an end-user to provide anonymous access to other services (please refer, as an example, to: http://www.thetop10bestvpn.com/). This is normally not a business service in the broader sense but a consumer service provided by CAPs to help end-users access contents (e.g. video) otherwise inaccessible (e.g. from another country...);

- A business service that connects several accesses of end-users and/or partners of a "business subscriber"[2]. This service may be implemented just as a closed user group or, additionally, provide a public access to the internet to (all or some selected) end users of the VPN.

A "business subscriber" has to be able to define which employees (the VPN end users) have access to internet services, as well as it must have the right to define which levels of internet access are to be granted to each employee or group of employees.

These access levels (sometimes defined, for instance, for security reasons, increased productivity and/or cost control) are of great importance in present days, and a relevant requirement in public tenders for medium/large companies. A few examples:

- Content filtering for video streaming services and other bandwidth intensive applications (e.g. bit torrent), that otherwise would slow down productivity across the company



- Security features for malware (Trojans, viruses, ransomware) prevention and detection (e.g. "Hackers have shifted their attacks to your network's weakest link: the user. They exploit the shortcomings of appliances by infecting your users when they visit trusted sites on the Internet. Hackers often attempt to hide attacks behind SSL-encrypted or CDN-delivered traffic", https://www.zscaler.com/why-zscaler/advanced-threat-protection)

[2] A "business subscriber" may include Member State's Public organizations

- Ensuring the highest encryption features that local hardware may not provide for the same cost (e.g. 2048-bit encryption algorithms, “RSA claims that 1024-bit keys are likely to become crackable some time between 2006 and 2010 and that 2048-bit keys are sufficient until 2030”, http://emc.com/emc-plus/rsa-labs/historical/twirl-and-rsa-key-size.htm)

- ISPs and other partners’ definition of the implementation details of business customers requirements.

These VPN services, considering their specific configurations and purposes, are surely outside the scope of the TSM Regulation and its spirit, in opposition to BEREC statements. The same applies, more generically, in what regards any restriction to the end-users’ freedom to contract the services that best suit their purposes. Any other interpretation would imply major competitive disadvantages for the European industry, namely:

- Commercial advantage for non EEA VPN providers and other ISPs (e.g. USA, China, Russia) which can provide these features to customers worldwide, namely through cloud services;
- European ISPs lack of commercial and technical flexibility to answer public tenders from medium/large size companies, due to prohibitions to comply with their requirements;
- Lack of European network innovation, namely regarding network virtualization and software defined networks;
- Poorer protection regarding cybercrime and terrorism.

BEREC needs to review the draft guidelines in order to overcome these illegitimate constraints, including the initial statements regarding VPNs, in order to comply with the end users and “business subscribers”’ rights and the security and integrity features required in the present days by society as a whole.

Thus, in what concerns VPNs, PT Portugal proposes the inclusion of these services in paragraph 12, at the same level of internal corporate networks or WiFi spots.

2. <u>Open internet access and commercial practices</u> (referring to Articles 3(1) and 3(2))

a) <u>The Network Termination Point (NTP) in the context of the consumer market and terminal equipment</u>

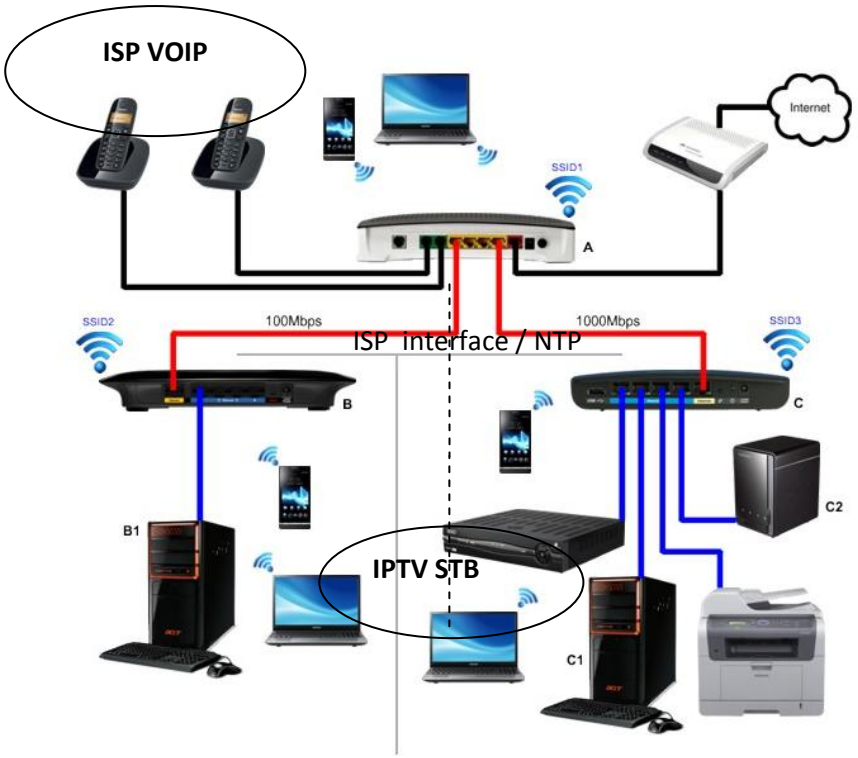
The Network Termination Point (NTP) is defined, in the Framework Directive, as the "physical point at which a subscriber is provided with access to a public communications network; in the case of networks involving switching or routing, the NTP is identified by means of a specific network address, which may be linked to a subscriber number or name".

It identifies the physical interface by which the ISP provides access to an "IP address: port number" with or without NAT implementations.

The fact that an ISP offer includes specific equipment to provide some SoIAS (e.g. IPTV or VoIP) must not be confused with the possibility the customer has to use other equipments (e.g. router) to connect to the ISP Home Gateway/router in order to get internet access with other characteristics, namely:

- other Wifi networking capabilities than those provided by the ISP (e.g. 802.11ac dual band 5Ghz/2,4Ghz versus 802.11n)
- other administration user interface e.g. for MAC address control, parental control, etc.
- other type of access to peripherals, e.g. printers, disks, etc.
- other remote access capabilities.

As an example, the overall customer network may look like the following:



We emphasize that the technological need for the router A to be provided by the ISP is directly linked to:

- the ability to provide, setup and operate the SoIAS services (e.g. IPTV, VoIP)
- the ability to provide, setup and operate the IAS in general
- ISP's O&M applications, including firmware/security upgrades
- WiFi capabilities for the ISP and the user (e.g. configuration of public hotspots)
- optional User Interfaces (UI) for the user (e.g. port forwarding, gaming, internet applications, servers, etc), some of which will be somehow virtualized in the network/cloud in the near future.

Thus, if an end user wants to use a different router A than the one provided by the ISP, the ISP cannot guarantee the adequate provision of the SoIAS, but will always be able to provide the IAS anyway.

In conclusion, in what regards terminal equipment for IAS, generally ISPs do not restrict consumer choice, provided that the equipment complies with the relevant standards and European Directives. However, in the case of bundles with SoIAS (e.g. IPTV services), many operators allow only the use of equipment provided in the package, in order to ensure the

correct operation of the service and its QoS. Additionally, some technologies (such as ADSL) require that the equipment used by the customer has to be certified. However, there may be constraints regarding the compatibility of the operating system of the users' terminal equipment with the use of certain applications, which is totally out of the control of the ISP, who cannot be held responsible for such restrictions.

All these aspects have to be taken into consideration when assessing guidelines on the users' terminal equipment.

b) Agreements between providers of IAS and end-users

BEREC guidelines should remain in line with the TSM Regulation and with general principles of the EU when assessing commercial practices and should not be so restrictive in what concerns the commercial offers allowed. In fact, it is undisputable from the TSM Regulation that NRAs' monitoring should only be done on an ex post basis, either on IAS commercial offers or services other than IAS, but the draft guidelines create uncertainties in that rule as they are unacceptably intrusive in some measures foreseen, including prohibiting per se some commercial agreements and offers, and thus should be reviewed on those aspects.

For instance, while the TSM Regulation allows ISPs to differentiate their retail offers based on parameters such as speed, price or volume, and such differentiation and business flexibility are essential to address the needs of customers, BEREC guidelines are further restrictive, namely under paragraphs 32 to 35.

In fact, according to article 3(2) of the Regulation, end-users have the right to agree on commercial and technical conditions and characteristics of the internet access service of their choice as well as, according to article 3(1), they have the right to use the content/applications/services of their choice, choose their terminal equipment and negotiate the conditions of their service. Choice is obviously a key concept throughout the Regulation (providing the agreements don't limit end-users' ability to choose what services can be accessed).

Additionally, “freedom of contract” has been recognised as a general principle of civil law by the European Court of Justice and has been seen as protected by article 16 of the EU Charter of Fundamental Rights, which states: “The freedom to conduct a business in accordance with Union law and national laws and practices is recognised.” Also, it has been clearly stated that « in business-to-business contracts [*where*] the principle of freedom of contract is paramount » (see. Green Paper on policy options for progress towards a European Contract law for consumers and businesses, 1 July 2010).

Therefore, at least in contracts celebrated with business customers, it is abusive to deny the parties the possibility of choosing the conditions of such contracts. In fact, all rules limiting the freedom of choice in contract matters should have the aim to protect at least one of the parties, and not, as it results from the restrictions now imposed by BEREC, prevent all parties from choosing deliberately the conditions of the services to be provided.

So restricting end-users’ freedom to chose, as established by BEREC, will prevent European businesses from agreeing with ISPs what best suits their needs and will give an unfair advantage to competitors located outside of the EEA, as, for example, in the US, where open internet rules only apply to consumers.

All in all, the lack of flexibility to accommodate end-users requirements goes against their freedom to choose the services they want to contract, and results in disadvantages particularly for business customers and their applications.

In fact, a business customer may want to:

- define target maximum bandwidth (e.g. file transfer) for certain applications in the public VPN access, which is unacceptable under BEREC’s draft guidelines as they consider this service as IAS;
- or even not to provide access at all to certain applications or protocols (e.g. to Social Networks), which is considered by BEREC as sub-internet service and forbidden under the draft guidelines.

End-users should be able to choose which types of applications, content categories of traffic and/or protocols they wish to access, the same way they should be able to choose which

ones they do not wish to access. These are the two sides of the same freedom. Therefore, ISPs should be allowed to keep offering commercial options that would enable end-users to access or not access applications or content according to their specific needs and choices, as the existence of contracts that include such type of restrictions specifically requested by the customer do not limit end-users' rights, quite on the contrary.

Another concern raised by the proposed Guidelines is the one that results from paragraph 75. It states that end-user terminal equipment-based restrictions are permitted, but not so if the same end-user asks for the ISP to provide those same restrictions in its network (unless the exception for reasonable traffic management is met). Despite being the same restrictions, resulting from a voluntary option from the end-user, somehow they end up being different solely on the basis of the technology where the restriction is implemented.

This interpretation is, at its best, discriminatory between technologies (network level vs terminal equipment level): comparable situations should not be treated differently and different situations should not be treated in the same way unless such treatment is objectively justified.

End-users should be able to ask for restrictions of access as long as they are duly informed of the consequences of such choice, and the ISPs have evidence of such demand from the customer. This should be allowed regardless of the technological means by which they are implemented.

Thus, the paragraphs which refer to restrictions put in place by end-users should be amended, allowing such practices, whether put in place by end-users themselves, or by the ISPs, if expressly requested by the customer. Prohibiting such practices would not take into account the specificities of end-user demands, including business needs, notably in terms of customised requirements.

It should be stressed again that one of the objectives underlying the TSM Regulation is the protection of end-user’s choices. It would be unacceptable to interpret and implement the Regulation in such a restrictive way that it would produce the opposite result of what is intended by the co-legislators and required of ISPs by a well functioning market

c) Zero-rating

While zero rated offers are considered negatively by BEREC in the draft guidelines, namely in paragraphs 37 to 45, the TSM Regulation does not even mention and much less prohibits per se such type of offers.

BEREC states that zero-rating practices could have different effects on end-users and the open internet, and hence on the end-users' rights protected under the Regulation. However, it is our belief that practices such as zero rating do not, in fact, limit the rights of end-users. Not only such type of offers can also benefit them but, additionally, these offers just reflect specific rules implemented at the level of traffic accounting, and do not involve technical differentiation at the level of the transport layer, such as guaranteed bandwidth allocation, nor limit end-users' choice.

Furthermore, the market is based on segmented offers and service providers must be free to make available a variety of price differentiated services in respect to the value of the offers. It should be recalled that price discrimination is a well known studied topic both in competition law and in economics and, except for certain situations where it can be deemed to constitute an abuse of dominant position, it is a welfare enhancing commercial practice as it increases the total output of a given industry.

As a conclusion, we consider that in case a given NRA considers there might be an issue with a commercial offer, it should check whether the conditions mentioned in Rec. 7 are fulfilled, namely if the commercial offer materially reduces end user's choices in practice, taking into account the market position of the IAS and CAP providers and if it undermines the essence of the end-users' rights. BEREC guidelines should only refer to those criteria without banning *a priori* certain commercial offers.

3. Traffic management (referring to Articles 3(3) and 3(4))

It must be understood that traffic management measures are critical: without them the internet does not work properly. Different types of traffic have different requirements and

the purpose of traffic management is the efficient use of network resources associated with the optimization of the overall quality and the best possible experience for end-users.

The TSM Regulation allows reasonable traffic management measures (art. 3, paragraph 3), and recital (9) links this concept with the optimization of the overall quality and user experience. Current practices fall within this concept, as they aim at the overall improvement of QoS (by which operators are evaluated by their customers). Thus, ISPs can use, and have to be able to continue to use, different types of traffic management mechanisms, depending on the critical issues: for example, the sensitivity of the traffic / application to the delay, the need for reaction to external causes (weather, congestion), etc.

Thus, the guidelines and the subsequent analyses by NRA should be based on principles and focus on traffic management objectives, particularly aiming to improve the customer experience. Quality segmentation between accesses of customers that have different QoS requirements (e.g. business customers) is a typical case to which the freedom provided by the Regulation should apply. The guidelines should also be flexible and future proof, in order to be able to adjust to innovation and the development of services and networks.

For instance, paragraph 51 mentions the congestion controls in the terminal equipment (allowed) vs controls in the network (restricted). How to reconcile this dichotomy with the progress we are seeing in the SDN/NFV, which involves increased equipment dematerialization and centralization of their functions in the network? This guideline is thus not future proof. Furthermore, such differentiation between what is allowed in the end-user's equipment and in the network layer seems to entail a violation of the technological neutrality principle.

Another source of concern is the need to adequately cope with emergency services and alike in the scope of IAS.

Additionally, strict compliance with non-discrimination must be carefully assessed: traffic of a given type doesn't always have a common technical identifier, so it is not realistically possible to ensure that it is treated exactly in the same way.

On the other hand, BEREC states that "In assessing traffic management measures, NRAs should ensure that such measures do not monitor the specific content (i.e. transport layer protocol payload). 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)." It should be clear that ISPs do not monitor specific payload content in terms of user information. But ISP have to be allowed to recognize information patterns in transport and application information. This may be the only way to correctly manage IP networks.

While it may be obvious, it should also be clear in the guidelines that certain traffic management practices must continue to be admissible at the request of customers.

As previously mentioned, business offers often involve specific terms agreed with customers (e.g. business customers wishing to block access to certain addresses/websites, content filtering, etc.), so these cases cannot be limited by the Regulation, as they would limit the freedom that customers should have to choose the way they wish to use the services provided by ISPs.

Thus, sections 52 and 75, among others, should have a safeguard in this regard and, additionally, the initial paragraph of the guidelines relating to Article 3 should state from the start that the guidelines do not restrict the freedom of customers and therefore do not apply to restrictions if expressly requested by the customer.

Most importantly, it is essential to be able to provide inside the Union the services that European customers require, otherwise they will migrate their services to non EEA platforms that are able to provide them with the specificities required.

More generally, if an IAS provider provides an option to the end-users by which they may choose to ban certain types of applications or specific content, e.g. child protection measures, ad-blocking, or access to certain categories of sites, it should not be considered as an impairment of freedom of choice of end-users. On the contrary, just like when end-users

voluntarily ask for the blocking of advertising content, it is an enhancement of end-users' choices and freedom. Therefore, BEREC should not prevent end-users from making personal choices and be entitled to obtain services that fulfil their requirements and needs.

At last, we want to emphasise that, as acknowledged by the Regulation, reasonable traffic management is necessary and cannot be replaced by increasing network capacity. And network dimensioning is a prerogative of the operator, who wants to offer the best possible services to its customers in a competitive environment, and should never be a mandate of the NRA, as seems to be the intention of the guidelines.

4. <u>Services other than IAS (SoIAS)</u> (referring to Articles 3(5) of the draft guidelines)

Co legislators have decided not to define and not to regulate services other than IAS (SoIAS), but BEREC's draft guidelines opted for an opposite approach and, in addition, even created a new non defined "sub-set" of services – "sub-internet services". In this respect, the draft guidelines go beyond the TSM Regulation and also pretend to reverse the burden of proof: according to the Regulation, SoIAS are allowed under certain conditions and it is for the NRAs to demonstrate (ex-post) when a given practice would not be in line with the Regulation.

BEREC should take into account that:

- SoIAS coexist with Internet access and contribute to the innovation of services and platforms. These are services different from the IAS and are optimized for content, applications or specific services that require QoS optimization and/or prioritization. For example, IPTV, VoIP, VoLTE; emergency services, ehealth, connected cars; services that address specific requirements of corporate customers, such as smart meters with QoS guaranteed and VPNs (note that, in our view, as previously mentioned, private networks should not be covered by the Regulation because they are not public networks for open Internet access).

- With regard to the ability of networks to provide SoIAS in addition to IAS, it should be noted that there are technologies such as ADSL, Cable or Mobile, which

require a commitment regarding capacity sharing between SoIAS and IAS, as it is not possible to increase the capacity.

- In order to ensure that both IAS and SoIAS are provided with consistent quality over time, usually an operator ensures adequate network dimensioning and additionally manages the traffic of certain services based on features and/or requirements like delay, packet loss or jitter. Thus, sharing and managing network capacity between IAS and SoIAS results in the global provision of better services.

- If there is an impact of SoIAS in the SAI provided to a customer (e.g. in ADSL accesses it may not be viable to ensure that the IAS will not be affected by SoIAS such as IPTV, particularly if the customer connects multiple simultaneous TV sets) this information should be transmitted to the customer in a clear but simple way, as it is now done.

Thus, all this section of the guidelines referring to Article 3(5) should be reviewed in order not to adopt a more restrictive approach on SoIAS than that which the TSM Regulation prescribes. Some non exhaustive examples follow.

Paragraphs 98, 104, 105 and 108 should be reviewed taking into account that the key principle of the TSM Regulation, as written in Article 3(5), is that providers "shall be free to offer services other than internet services" under specific conditions. This acknowledgment of ISPs freedom to provide SoIAS should be the starting point of BEREC analysis. Therefore any assessment of those types of services can only be done ex-post by NRAs which have to prove that the specific conditions required for the provision of SoIAS have not been met. BEREC final guidelines should explicitly mention that this assessment is "ex-post" as the current proposed wording reverses the burden of proof.

It cannot be ignored by BEREC that provisions (such as "strict admission control", "logically separated from the IAS") which have been explicitly rejected from the Regulation during the legislative debates should not be reintroduced in the BEREC guidelines (e.g. paragraph 106). During the legislative debate, it was explicitly decided not to define or characterise the so called "specialised services" to avoid obsolete or non future proof definitions.

In what regards paragraph 115 and 116, it has to be understood and made clear that the appreciation of the required QoS level for a given service shall remain the sole responsibility of the ISPs and not be subject to arbitrary administrative control. Otherwise, it would harm consumers' choice, by being deprived from the benefit of competition between providers of quality services.

For instance, it should not be up to an NRA to decide whether the provision of an ADSL2+ line for 8 Mbps allows the availability of an IPTV plus VoIP SoIAS: considering that any HD channel for a single box will use ~4 Mbps, the NRA is not really entitled to decide if the remaining 4 Mbps are enough for IAS and it is doubtful, in any case, if NRAs are technically prepared to make such assessments.

We consider that this kind of evaluation should be done at the portfolio level and at the technical level, and it should not be forgotten that ISPs provide services in a highly competitive environment and thus that it is in their best interest to offer the best possible services to their customers.

5. **QoS measures, transparency and monitoring system's certification** (referring to Article 4)

a) QoS measures, transparency

We consider that the draft guidelines don't answer several critical issues: they don't define what QoS is (only partially, speed), nor detail how it should be measured. Additionally, they don't take into account all the constraints that may influence QoS and that are out of the control of the ISP.

For instance, TSM Regulation does not define (ISO or Internet) layering choices in speed determinations neither protocols (TCP and not UDP...). It just refers that measurements should be performed beyond the "ISP leg", an expression which is prone to misunderstandings. In this respect, we propose adding to paragraph 163 of the draft guidelines "in national territory and within the ISP's sphere of control", to make it clear.

Additionally, and still in what regards speed, it is necessary to take into account that such measure is substantially dependent on the technology of the access network and many other factors outside the control of ISPs, and it is not viable to customize such information on a end user per end user basis; instead, reference to ranges must be allowed. Also, providing coverage maps comparing estimated and measured values at each location both indoor and outdoor, would be so difficult to achieve, that the end result would be serious misinformation for end-users.

On the other hand, the regulation implies new requirements in terms of information to be published and included in contracts (regarding traffic management measures and download and upload speeds) that leads to undesirable complexities, including for end-users.

We believe that the information provided to end-users should be simple and easily understood, and that NRAs must take a suitable compromise between ensuring transparency and burdening end-users and ISPs with complex technical parameters, also taking into account that it would be neither justified nor proportionate to impose on ISPs the dissemination of detailed technical information that is not beneficial nor understood by end-users.

It is important that ISPs are allowed flexibility to find the best way to deliver these informational elements in a clear and understandable approach for end-users (using, for example, multimedia educational content available on a website, instead of including detailed technical explanations in the supply of the services and contracts).

It is our understanding that TSM Regulation most important rules and aim are:

- Transparency on the speed to be expected under normal conditions and criteria for its determination
- Simple explanations to users
- Clear dispute resolution
- Freedom for an informed choice by the user.

But in the draft guidelines BEREC is defining and thereby restricting what could be considered a transparent mean to explain users which speeds are to be expected according to the service provided and how they should be measured.

On the other hand, regarding clear dispute resolution, the Regulation does not state the need for the ISPs to have a specific customer service for addressing only issues regarding complains about open Internet rights and obligations. Therefore, we cannot understand why BEREC found the need to create such obligations, considering the fact that ISPs already have in place effective and widely advertised complaint services.

In our view NRAs should only be concerned with the following:

- Is the information provided to the customer simple and clear?
- Is it measurable by the user, using a certified mechanism?
- What should be the remedies imposed on ISPs if the measured speed is systematically below the contracted speed? (In any case, ISPs should not be penalized for an eventual non-compliance before being defined robust measurement concepts and methodologies, respecting a reasonable period of adaptation).

b) Monitoring system's certification

In what regards QoS monitoring systems, the draft guidelines are inconsistent with the TSM Regulation in what concerns the requirement for their certification, namely in paragraphs 158 and following. In fact, while the regulation states in Article 4(4) that any significant discrepancy between the actual performance of the IAS and the performance indicated by the ISP shall be deemed to constitute non-conformity "where the relevant facts are established by a monitoring mechanism certified by the national regulatory authority", the draft guideline §158 refers that "The Regulation does not require Member States or an NRA to establish or certify a monitoring system". Thus, this must be amended.

Additionally, the draft guidelines are inconsistent in themselves, as they define, in paragraph 162, the methodologies that NRAs should follow to guarantee the consistent application of the TSM Regulation while, in paragraph 160, they allow NRAs to use their existing

measurements tools, even if they don't follow those methodologies. Due to the critical issues that can be raised by the results of measurements, including monetary compensations, this is an unacceptable situation and we consider that all monitoring measurement systems that can be used to evaluate the performance of ISP vis-a-vis the contracted conditions have to be duly certified according to well defined rules.

And it is absolutely necessary that the speed monitoring mechanisms to be certified by the NRAs exclude factors that influence the performance of the IAS and that cannot be controlled by the ISPs, such as the type of terminal equipment, software used, the type of the home network access (physical or wi-fi), the number of equipments it hosts, etc., as well as the number of simultaneous users and the distance to the mobile cell in case of mobile services.

6. <u>Supervision and enforcement</u> (referring to Articles 5 of the draft guidelines)

In the framework of its responsibility of supervision BEREC should not add to the general workload of BEREC itself and of the ISPs by asking too much (and unreasonable) information and set up excessively heavy processes. Time is key for operators to efficiently manage their networks and to offer innovative services and this should not be undermined by over prescriptive administrative and bureaucratic processes, both for ISP and NRAs.

We believe that the draft guidelines foresee a non proportional and unacceptably intrusive regular reporting and ex-ante measures (for instance, in what regards commercial agreements), which should only be justifiable ex-post following an evidence based complaint or market failure.

In fact, there are several paragraphs of the draft guidelines (e.g. from 86-89) suggesting a very pro-active and interventionist role of the NRAs in controlling traffic management measures implemented by operators. While it is true that Article 5 of the TSM Regulation gives NRAs the powers to monitor and ensure compliance with the Regulation, the exercise of these powers is not exempt from the observation of the principles of necessity, appropriateness and proportionality, which should guide the action of the NRAs.

We note that the draft guideline 177 already defines (and rightly so) that the imposition of measures to ISPs is subject to the application of those principles, but doesn't make clear that also all the effort to collect information must also be weighted and justified by national circumstances, and subject to concrete evidence or justified suspicions that there are violations of the TSM Regulation in what regards traffic management measures.

We consider that the guidelines should make clear that NRAs must carry out the monitoring measures provided for in the TSM Regulation, and proceed with the collection of the necessary information, only when they consider that this is justified in order to ensure compliance with the TSM Regulation. Thus, we suggest that the relevant guidelines should begin with the words "When deemed necessary in light of national circumstances, NRA..." or some equivalent text.

On the other hand, in paragraphs 88 and 89, and also in 115, the draft guidelines go as far as prescribing that the NRAs should evaluate whether other exceptional congestion management measures would be preferable to operators, if the throttling would be preferable to blocking, if the networks are properly sized. The market reality underlying these guidelines is clearly different from what we experience in Portugal (and in the Union, in general). This level of intervention and interference in the way operators manage and optimize their networks can only be admitted in a market performing very badly, without the competitive tensions that endogenize the race for continuous improvement of networks and the services provided.

Also, as stated before, network dimensioning is (and should always remain) a prerogative of the operator, who wants to offer the best possible services to its customers in a competitive environment, and should never be a mandate of the NRA. It is inconceivable that ISPa may be subject to such a level of control and intervention and we believe these procedures would go far beyond the objectives of the TSM Regulation.