BEREC Guidelines
on the Implementation of the Open Internet Regulation

Consultation response

Introduction

This submission is supported by 23 digital rights NGOs and contains suggestions for the ongoing consultation of the BEREC Guidelines on the Implementation of the Open Internet Regulation (Regulation (EU) 2015/2120, "the Regulation"). We would like to thank BEREC for the invitation to the Stakeholder Workshop on 29 May 2019 in Brussels and reference our written submission on this occasion[1]. This submission contains further responses to the draft text of the new Guidelines published by BEREC.

Parental Controls and End-Point Based Blocking

Paragraphs 32a-b and 78-78b introduce language specifying that blocking of particular content, services, or applications is to be assessed under Article 3(2) of the Regulation. The consultation document calls these changes 'clarifying', however we consider them to instead blur the issue, and the application of Article 3(2) to these products to be misguided. The legislative history clearly shows an intentional choice not to allow parental control filters in the provision of IAS in the Regulation, as an exception allowing such measures was removed in the trialogue negotiations. Concerns regarding other IAS with blocking functionality other than for the purpose of parental control are analogous to those regarding parental control filters.

Article 3(3) of the Regulation prohibits the filtering of traffic (subject to the exceptions not applying in the case of the filtering products concerned) 'when providing internet access services'. Yet, the new paragraph 78b seeks to restrict the application of Article 3(3) so long as a filtering product is 'end point-based' and offered in a 'similar' way to filtering products offered by third-party CAPs. The redirection of traffic to filtering DNS servers or HTTP proxies by accordingly configured terminal equipment are mere 'examples' of such products, leaving the question of what consists of an 'end point-based' filtering service open to interpretation and case-by-case assessment.

This language is less clear than the distinction made in paragraph 78 of the current Guidelines, distinguishing between 'network-internal blocking' and 'terminal equipment-based restrictions' put in place by the end-user, a distinction supported by the stated scope of Article 3(3). When a filtering product that performs network-side filtering is sold in conjunction with an access product (perhaps even as a default), and is only usable by subscribers of said access product, the subsequent filtering clearly takes place 'when providing internet access services'. Article 3(3) applies to these products, and no case-by-case assessment as to the price of the product or the configurability by the user, as suggested by paragraph 32b, is necessary.

If IAS providers want to provide filtering services, these fall outside of the scope of the Regulation if these services are not part of an access service, i.e. if they are provided not merely 'similarly' to third-party CAPs, but in the same way as third-party CAPs. In particular, the filtering service must be offered as a clearly separate and optional service from the IAS itself, in the same way as filtering

1 https://epicenter.works/document/2013

services from third-party CAPs. Moreover, the installation and/or configuration of the filtering service must be actively done by the end-user on the relevant client devices (e.g. computers or tablets) or terminal equipment (e.g. configuration of an access router). The filtering service cannot be automatically provisioned to the end-user by the IAS provider, e.g. provisioning of a DNS resolver via DHCP, since this would effectively constitute blocking in the part of the network over which the IAS is provided, and would conflict with the requirement that the service is offered in the same way as filtering services from third-party CAPs. We welcome the clarification in paragraph 78a that the primary DNS resolver, which we understand to be the one that is automatically provisioned in the network to the end-user by the IAS provider, is an inherent part of the IAS and must comply with Article 3(3).

If the filtering service is offered in this manner, the service is not in the scope of Article 3 of the Regulation, and no case-by-case assessment under Article 3(2) is to be made.

Therefore, any assessment of such services is an assessment of whether the service is in scope of the Regulation, and not an assessment under the Regulation. If filtering services come in scope of the Regulation, they invariably by their nature constitute restriction or interference according to Article 3(3).

We therefore consider the language of paragraphs 32a-b, subjecting these products to an assessment under Article 3(2), and the language of paragraph 78b misguided. BEREC should delete paragraphs 32a-b and the language of paragraph 78b from 'However'.

No Circumvention of Non-Discrimination Provisions by Agreement

Paragraph 37 brings much needed clarity on one of the core questions of regulatory enforcement of the Open Internet Regulation in the past years. It is vital for BEREC to provide guidance on such an elementary question. We very much welcome the amendment to this paragraph and strongly argue in favour of it.

The structure of the Regulation would collapse if one were to take the view that Article 3(3) only applies where a subscriber has not agreed to traffic management that is not 'reasonable' as per Article 3(3), second subparagraph, of the Regulation. Article 3(3) imposes a general non-discrimination obligation that applies to all treatment of traffic irrespective of any individual IAS, but on all internet access services (*plural*). Furthermore, commercial considerations are specifically excluded as a basis for reasonable traffic management measures. This view has been confirmed by the Higher Administrative Court of Münster.[2]

5G and Regulatory Assessment of Network Slices

We welcome the additions in paragraphs 34 and 34a-c. The particular focus on application agnostic provision of IAS ensures the protection of end-user rights according to Article 3(1).

We particularly welcome paragraph 34b as it provides an essential safeguard, ensuring that upcoming provisioning of 5G networks is not to the detriment of existing IAS subscriptions. Because of the high transmission speeds that 5G networks promise, the backhaul and backbone capacity of IAS providers could become a bottleneck in the near future. Therefore, BEREC is right in highlighting that existing contractual obligations are to be upheld. Yet, we caution regulators that the extent of these

2 Decision 13 B 1734/18, para 33 ff. http://www.justiz.nrw.de/nrwe/ovgs/ovg_nrw/j2019/13_B_1734_18_Beschluss_20190712.html

obligations is often not clearly specified as many IAS contracts only specify some of the criteria required by Article 4(1) and often do so only vaguely and without a clearly specified assessment methodology. It is therefore vital that NRAs follow BEREC's guidance in this paragraph and make use of their power to impose requirements according to Article 5(1) concerning older access technologies that may no longer be in the economic focus of the IAS provider but still serve many customers.

We very much welcome paragraph 34c as it provides much needed clarification on the crucial question of how to assess new access products.

In order to bring the potential of 5G networks to fruition it is necessary that they provide a user-controlled environment that empowers citizens to make use of differentiated network qualities in a way that suits their needs.

Any preselection or reclassification by IAS providers of the network slices used by a particular application or service would have to be assessed under Article 3(3) of the Regulation. This paragraph applies generally to the provision of internet access services. Subparagraph 1 creates the obligation to treat traffic equally irrespective of content or application. Subparagraph 2 subsequently prohibits any differentiated treatment of applications or services based on commercial considerations, which includes access products providing multiple levels of quality.

Any interference by IAS providers regarding which quality level is used for which application, content or service violates the end-user rights of Article 3(1). Given that the right to access and distribute information regardless of content, application, or service is directly linked to one particular internet access service, no agreement with an IAS provider can limit the end-user choice of which application is to make use of which quality level within a subscription.

The assessment of user control in such products is therefore essential and we propose an appropriate strengthening of the language in paragraph 34c:

> 34c. If IAS offers come to the market which facilitate multiple QoS levels at the same time for a single subscription, NRAs should note that this may be allowed as long as this practice is application-agnostic and is in line with the requirements in Articles 3(1) and 3(3). In such an assessment, the NRA **shall**~~may~~ among other factors take into account that end-users must have full control over which applications transmit traffic over which QoS level (e.g. by configuring the client application software) and that the QoS level in which specific applications are transmitted is not preselected by the ISP (e.g. based on commercial agreements with CAPs or the other end-user). Such assessment procedures could be fine-tuned by the NRAs if and when new use cases are implemented by ISPs.

Differential Pricing Practices

We would like to reiterate our position that in our reading of the Regulation differential pricing practices and zero-rating in particular are prohibited as violations of the general non-discrimination clause of Article 3(3), first subparagraph. However, given BEREC's contrary view, we would like to propose improvements to the draft rules.

We welcome the additions to paragraphs 40 and 42. It is important for BEREC to offer a clear nomenclature for the phenomena which have to be assessed according to the Regulation. However, we would have preferred the term "differential pricing practices" instead of "zero-rating". This term is

used in Canada and India and covers the whole range of practices, including zero-rating or application-specific data volume.

We welcome the addition of paragraph 42b. It is important for BEREC to establish a clear set of rules and to ensure that it is applied by NRAs. Right now this is not the case. Most NRAs do not stringently follow BEREC's assessment criteria. Gaps in the consideration of assessment criteria have led to zero-rating products continuing to be offered even where they run counter to the aim of the Regulation of guaranteeing the continued functioning of the internet ecosystem as an engine of innovation. As BEREC now defines in more detail under which circumstances open programmes can be considered allowed, it also urgently needs to draw a red line where that do not meet these criteria and that should be considered to contravene the Regulation.

We therefore propose a strengthening of the language of paragraph 42b:

> 42b. When assessing zero rated offers and/or programmes, NRAs **shall~~may~~** consider the extent to which the programme meets what BEREC would consider best practice by being open to all CAPs of a particular category and, for open programmes, whether the terms on which CAPs may join the programme are transparent, non-discriminatory, fair and reasonable. **When a programme is in breach of these best practices, it likely undermines the essence of end-user rights according to Article 3(1) of the Regulation.**

We welcome paragraph 42c. It hints at much needed transparency for consumers on which particular aspects of an application are excluded from the general data volume, however, if transparency is to serve as a protection of end-user rights according to Article 3(1), this transparency cannot be optional as it forms the basis of any informed decision-making by the consumer or a CAP designing their offer. We therefore propose the following changes:

> 42c. When assessing whether the terms for joining an open zero-rating programme are transparent, NRAs **shall~~may~~** consider the extent to which they are publicly available, as well as the availability of the ISP's contact details, and the procedure and regular timeframe for processing request to join the programme. NRAs **should~~may~~** also consider whether the process for CAPs to apply to join a programme is straightforward, e.g. via a standardised online form on the ISP's website, and whether a list of participants to the programme is publicly available. Transparency for end-users as to which content provided by a CAP in the programme is zero-rated and which is not **needs to be provided by the IAS provider before and the end-user enters into the contract~~may also be relevant~~**. For example, if the music content of a particular music application is zero-rated but data used for advertising in that application is not zero-rated, this should be clearly explained to the end-user, at a prominent place and before the end-user decides to use the application.

We welcome paragraphs 42d and 42e. They provide clarity and complement the framework.

We welcome the first bullet point added to paragraph 48, but wish it went further. It is important to tie the proposed ruleset on best practices for open programmes to concrete regulatory enforcement actions against offers not meeting these standards. BEREC's interpretation of the Regulation in this area has proven impactful on market developments in the past.[3] Before the 2016 Guidelines, open programmes were almost not present in the European market at all. Yet, three years after the rules

3 We attribute the increase in open programmes to paragraph 46, fourth bullet point, of the 2016 Guidelines.

were adopted, 66% of zero-rating offers are still closed and offer no contact information for interested CAPs.[4] We caution BEREC that the proposed draft Guidelines will only perpetuate this situation and not lead to an improvement if red lines are not drawn.

We would like to point out the corresponding research taken out by epicenter.works and published in a Jauary 2019 report[5].

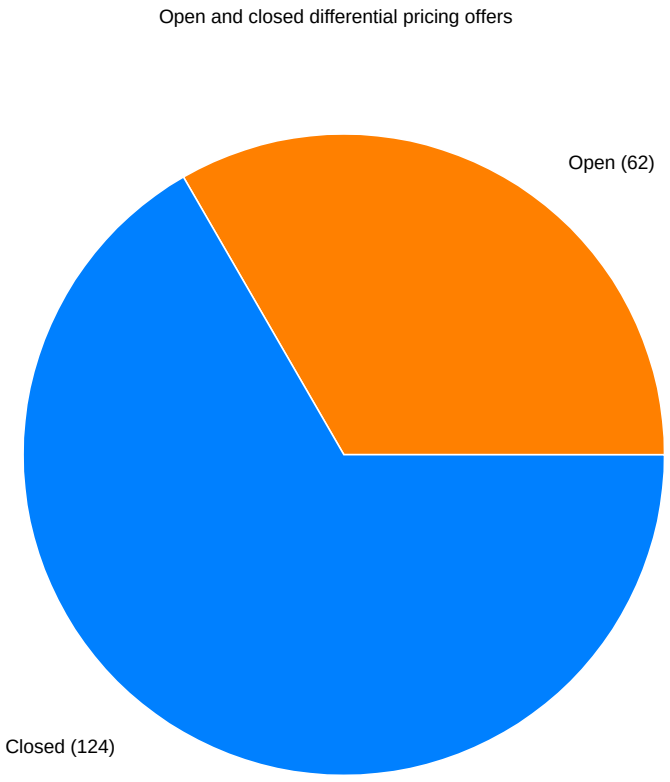

Illustration 1: Distribution between open and closed differential pricing practices

Prohibition of Deep Packet Inspection Practices for IAS Providers

The consultation document calls into question the privacy safeguards against deep packet inspection technologies in paragraphs 69 and 70 of the Guidelines. These paragraphs detail the monitoring prohibition of specific content in Article 3(3) subpara 2 of the Regulation. According to statements at the public debriefing on outcomes of the 40th BEREC plenary meeting in Brussels on 10 October 2019[6], the suggestion has been made that IAS providers should be allowed to inspect domain names in users' communication data as part of traffic management measures they employ.

4 See page 18 of the Report: The Net Neutrality Situation in the EU of epicenter.works based on a complete survey of differential pricing offers: https://en.epicenter.works/document/1522

5 https://en.epicenter.works/document/1522

6 See https://www.youtube.com/watch?v=rvvg2325vtc

However, the current distinction between specific an general content made by the Guidelines is the correct one. The provision of IAS as such, i.e. the relaying of traffic generated by or destined to subscribers, does not require the processing of transport layer payload. The suggested processing of such data to distinguish particular service providers from other providers of the same type of service (by distinguishing traffic communicated to hosts determined by the owners of particular domain names) cannot be "non-discriminatory" as required by Article 3(3), second subparagraph, and the prohibition on monitoring of specific content must be read as giving effect to this restriction in terms that protect the privacy of subscribers' communications. Domain names are therefore to be considered specific content.

Question 1

> *1) Are you aware of any IAS which operate "specific categories of traffic" (ref. Article 3(3)) on the market, and if so which categories are defined? For ISPs: If you have implemented traffic categorisation in your network, please explain which technical quality of service requirements these categories are based on.*

As transparency statements by IAS providers are vague and the detection of traffic management by means of measurement requires large, distributed efforts, we are currently not securely aware of such traffic management measures that BEREC is not already aware of through NRA action and past litigation. We suggest that NRAs use their Article 5(2) powers to create a comprehensive list of such measures employed by IAS providers. To implement class-based traffic management IAS providers can resort to distinctions based on port numbers, IP addresses, other IP header information such as the ToS header field, and size and frequency of data packets. Using DPI for this purpose would be disproportionate.

Question 2

> *2) Please explain in detail which methods exist and which of these methods are used in practice for traffic identification for billing purposes (in particular zero rating) and for traffic categorisation for traffic differentiation purposes. For ISPs: If you have implemented any of these methods in your network, please explain why the particular methods have been chosen. Please give concrete examples.*

Based on our reading of technical and commercial documentation of differential pricing products in the EEA we can identify four types of markers used to identify traffic of participating CAPs:

1. **IP addresses:** This method is the least privacy intrusive, but requires the CAP to host its service using dedicated IP addresses. When the service is delivered by shared servers or via a CDN this may not be the case.
2. **DNS Snooping:** This method is used by the Vodafone Pass zero-rating offer. This presumably refers to the inspection of subscriber DNS traffic in order to continuously learn IP addresses whose traffic is to be treated distinctly.[7]

   DNS snooping is not possible if DNS-over-HTTPS (DoH) or similar techniques are used. Mozilla and Microsoft plan to enable DoH for their users.
3. **Server Name Identification (SNI):** This method uses the domain names transmitted in the clear when initiating encrypted connections. The privacy impact of identifying domain names

7 See e.g. the documentation of Cisco ASR 5000-series products.

can be severe as it can reveal sensitive information about the user when they access services provided by health services, political parties or religious communities.

SNI can be used for traffic identification only if the TLS handshake is not encrypted. Encrypted SNI for TLS 1.3 is not yet an Internet standard, however, there has been experimental support by e.g. significant CAPs and browser vendors Cloudflare and Firefox since 2018. Furthermore in the case of services offered over HTTPS, SNI identification relies on the identity of SNI information and the unobservable (encrypted) HTTP host header, which need not coincide in the case of certain cloud hosting services and CDNs.[8]

4. **Uniform Resource Locators (URL):** The identification of traffic to be zero-rated according to URL is advertised by multiple zero-rating programmes. URLs identify specific resources on the web and specific API functionality of applications. The privacy impact of processing URLs is potentially enormous as such information reveals detailed user behaviour: in many cases, there is a direct correspondence between a URL and concrete content (e.g. a specific image, a specific blog article, a specific video segment) or concrete service functionality.

   In order to use URLs for traffic identification, it is necessary that the traffic is transmitted unencrypted.

Question 3

> *3) Is it possible to identify traffic for billing purposes and for traffic categorisation using the techniques mentioned in BEREC GL paragraphs 69 and 70 and are there practical differences between the different use cases (billing/traffic categorisation)? Please explain why you believe the current Guidelines are sufficient or not by providing concrete examples.*

The identification via SNI and URL criteria is based on the monitoring of specific content and therefore cannot be in line with any meaningful reading of the Regulation. Therefore, we strongly argue in favour of the current version of paragraphs 69 and 70 and see no reason to amend them. They offer clear guidance to all parties involved, in particular with regard to subscribers' expectation on the processing of their personal data when using IAS.

The question of rephrasing paragraphs 69 and 70 is the result of novel commercial practices by IAS providers based on Article 3(2). As BEREC has noted in paragraph 37 of the draft Guidelines, agreements and commercial practices based on this Article 3(2) do not relieve IAS providers from the obligations of Article 3(3).

Question 4

> *4) For End-Users: Do you feel informed about reasonable traffic management measures and the methods used for the identification of traffic? Please explain.*

According to the assessment of EDRi and the EDRi network, consumers are provided with very little to no information on the privacy impact of differential pricing practices. No agreement that we could evaluate satisfies the requirements for informed consent. In most cases there is no mention at all of the processing of personal data to provide such a service.

8 The technique of using differing SNI and HTTP Host headers is called "domain fronting".

Even if one takes the view that informed consent of customers can solve this issue, it is still insufficient to remedy the issue of processing of information from non-consenting third parties communicating with users of such offers.

Sadly, we also see a widespread failure by IAS providers to adhere to Article 4(1) of the Regulation. Although there have been cases where Article 4 was enforced by regulators in the context of differential pricing practices, to our knowledge no such case has scrutinised the transparency obligations regarding the privacy impact of such offers. BEREC should therefore give further guidance on this issue regarding the implementation of Article 4(1) (see below).

Specialised Services

We want to stress the importance of paragraphs 101, 105 and 111 on the important obligation of NRAs to ensure that any quality assurance of speicalised services is objectively necessary given the technical characteristics of the underlying content, application or service. Once a service can function over the open internet, it should not qualify as a specialised service.

We understand the amendments to paragraphs 108, 108a, 109, 110, 110a and 110b as necessary adaptations that provide further guidance. Yet, we would like to highlight that paragraph 110a also describes the connectivity model that could for example be used for a Netflix or Youtube specialised service.

We support that BEREC acknowledges in paragraphs 111 and 112 that the provision of specialised services is dependent on the current IAS quality levels and therefore the obligation of NRAs to verify if the optimisation is objectively necessary is not static, but has to be evaluated over time.[9]

However, we are concerned about the amendment of paragraph 112. The damage done to consumer choice and competing services when specialised services are given priority over comparable content reachable over the IAS should not be assessed only once every several years and then prolonged with an extensive transition period. The purpose of the Regulation to protect the internet as an engine of innovation is not compatible with inactivity by NRAs, and changing circumstances may require fast intervention by NRAs to ensure a competitive market in particular applications or services. The rapid development of service provision on the internet requires the opposite approach: NRAs must be able to reassess services whenever proportionate, so as not to unjustifiedly disadvantage new service providers competing with an established service currently classified as a specialised service.

112. 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 objectively necessary, 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. NRAs should assess whether a service qualifies as a specialised service on a case-by-case basis. ~~**In case of reassessment, this would be expected to take place over a larger timescale, usually several years.**~~ NRAs are ~~**not**~~ expected to keep specialised services **and comparable content, applications or services available via the internet access service** under constant review. When an NRA assesses that a service that no longer qualifies as a specialised service due to the improved quality of IAS, the ISP should be allowed a ~~**reasonable**~~ transitional phase for phasing out of the specialised service**, which takes into account the damage done to**

9 We have argued this point in our 2016 submissions. https://en.epicenter.works/document/1102 and https://en.epicenter.works/document/346

comparable services. In these circumstances, national administrative and procedural laws apply, including observing the principle of proportionality.

We welcome the clarification in paragraph 115.

We are very concerned about an amendment to paragraph 121 which restricts the safeguard against quality deterioration through specialised services to the same network they are provided over. This reading ignores the technical reality of shared backhaul and backbone capacity between different access technologies, in particular mobile network generations. Particularly in light of 5G, it is likely that the bottleneck of ultra-fast last mile technologies will become the backhaul and backbone. Newly provisioned specialised services via 5G technology could therefore lead to a deterioration of IAS quality of 3G and 4G networks.

In all places where the Regulation provides a safeguard against quality deterioration, this safeguard is specified without a restriction to a specific network, but the IAS overall. We therefore argue this amendment to the Guidelines is not in line with the Regulation and should not be adopted by BEREC.

Additionally, we ask BEREC not to weaken the language on the enforcement of this vital safeguard. Assessing the potential quality deterioration of IAS through the provisioning of speicalised services can only be done with a historic comparison of IAS performances of particular networks. According to a 2019 study conducted by epicenter.works, only 8 out of 32 NRAs fulfilled their obligation in 2017 or 2018 to measure the quality of the internet in their country and also report these numbers in their annual report, as specified in paragraph 183 of the Guidelines.[10] Clearly some regulators acknowledge the need to assess current quality levels in their country and also report on these numbers to the public. With the expected increase in provision of specialised services it is important that NRAs have this historic data on quality levels at their disposal to assess whether the quality of the IAS is deteriorating. Ensuring an increasing quality of the IAS is not a luxury exercise, but one of the core missions NRAs are tasked with under the Regulation. Hence, we are worried by BEREC's attempt to further weaken the language in paragraph 121. Contrary to the BEREC draft, we suggest a tightening of the language to ensure that the quality levels of IAS as a whole are assessed by regulators and transparently reported.

121. Specialised services are not permissible if they are to the detriment of the availability and general quality of the IAS ~~offered over the same network~~. There is a correlation between the performance of the IAS offer(s) (i.e. its availability and general quality) and whether there is sufficient capacity to provide specialised services in addition to IAS. NRAs **should**~~may~~ consider that IAS quality measurements **have to**~~could~~ be performed with and without specialised services, both in the short term and in the long term, which **should**~~may~~ include measurements before the specialised services are introduced in the market as well as after.

We welcome the reference in paragraph 121a to the BEREC measurement tool and hope that NRAs adopt this tool in their respective member states.

10 See page 12 of Report: The Net Neutrality Situation in the EU https://epicenter.works/document/1522. The only 8 countries fulfilling this reporting obligation in 2017 and 2018 were Austria, Estonia, Norway, Poland, Romania, Slovak Republic, Sweden and the United Kingdom.

We agree with most of the changes in paragraph 124. However, the Regulation protects all end-users and not just the majority of them from quality deterioration of their IAS by specialised services. Therefore, we suggest to remove the "number of users affected" as an assessment metric.

124. NRAs could assess whether the provision of specialised services reduces general IAS quality, for example, by assessing the extent to which measured download or upload speeds are lowered or delay, delay variation or packet loss are increased ~~and the number of users affected~~. 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.

We do not agree with the amendment of paragraph 125. A "perceptibility" test is unnecessarily subjective and contradicts the objective language of statistical significance and consistent performance degradation in this paragraph.

125. NRAs should intervene if persistent ~~perceptible~~ 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.

Transparency Obligations

We welcome paragraph 135 as it provides much needed clarity for end-users. Transparency about the implications of the wide-spread practices of zero-rating and congestion management is much needed. We suggest a further clarification on the privacy implications of the use of identification technologies.

135. NRAs should ensure that ISPs include in the contract and publish a clear and comprehensive explanation of traffic management measures 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;. In particular the following information should be provided by the ISP:
  - the download and upload limits or data usage caps that apply to the internet access service selected by the end-user, the traffic management used to manage compliance with data caps and download limits, and the circumstances under which these apply.
- the circumstances and manner under which traffic management measures possibly having an impact as foreseen in Article 4(1) (a) are applied;
- how the measures might affect QoS of the internet access service, particularly in cases of network congestion and also in relation to other internet access services with different QoS parameters where multiple internet access services with different QoS parameters are offered by the ISP

- 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. **This includes in particular identification technologies for the purpose of application specific billing (zero-rating) and traffic management measures based on specific content.**
- Any traffic management measures defined in a contract should be as specific as possible in their information.

We very much welcome paragraphs 141, 141a and 142, as they provide an important clarification for new hybrid IAS technology.

We welcome the clarifications in paragraphs 164 and 165.

Supervision and Enforcement

We suggest that BEREC amend paragraph 184 to clarify that NRAs have the mandate to inquire about the type of information they need for the ex-post evaluation of zero-rating products which has been specified in paragraphs 42b, 42c, 42d and 42e.

184. NRAs may request from ISPs information relevant to the obligations set out in Articles 3 and 4 in addition to the information provided in contracts or made publicly available. The requested information may include, but is not limited to:

- more details and clarifications about when, how and to which end-users a traffic management practice is applied;
- justifications of any traffic management practice applied, including whether such
- practices adhere to the exceptions of Article 3(3) (a)-(c). In particular,
  - regarding Article 3(3)(a), the exact legislative act, law, or order based on which it is applied;
  - regarding Article 3(3)(b), an assessment of the risk to the security and integrity of the network;
  - regarding Article 3(3) (c), a justification of why congestion is characterised as impending, exceptional or temporary, along with past data regarding congestion that confirms this characterisation, and why less intrusive and equally effective congestion management does not suffice.
- requirements for specific services or applications that are necessary in order to run an application with a specific level of quality;
- information allowing NRAs to verify whether, and to what extent, optimisation of specialised services is objectively necessary;
- information about the capacity requirements of specialised services and other information that is necessary to determine whether or not sufficient capacity is available for specialised services in addition to any IAS provided, and the steps taken by an ISP to ensure that;
- information demonstrating that the provision of one or all specialised services provided or facilitated by an ISP is not to the detriment of the availability or general quality of IAS for end-users;
- details about the methodology by which the speeds or other QoS parameters defined in contracts or published by the ISP are derived;
- details about any commercial agreements and practices that may limit the exercise of the

rights of end-users according to Article 3(1), including details of commercial agreements between CAPs and ISPs;
- **details on the admission procedure of zero-rating programmes, like duration of the procedures, conversations with CAPs that have not entered into the admission agreement and technical efforts undertaken to identify participating applications;**
- details about the processing of personal data by ISPs;
- details about the type of Information provided to the end-users from ISPs in customer centres, helpdesks or websites regarding their IAS;
- the number and type of end-user complaints received for a specific period;
- details about the complaints received from a specific end-user and the steps taken to address them.

Annex

In general, we welcome the step-by-step assessment of zero-rating and similar offers.

Point 2(a)(i) of the annex lists several metrics of comparison between application-specific and agnostic modes of IAS. However, the metric most relevant to users of particular applications over an IAS, the cost per usage duration of an application or service, is missing from this list. In order to assess the impact of agreements and commercial practices on the end-user right to access and offer services, the possible duration of usage of these services is therefore highly relevant. We propose to add this in a specific subitem to Point 2(a)(iv).

iv. The comparison of usage duration of an application or service that is priced differently from competing applications or services accessed via the IAS: Does the difference in usage duration constitute distort competition in favour for the zero-rated application? Can the end-user use the application for typical lengths of time with a non-zero-rated application or is freedom of choice restricted?

Finally, we ask BEREC to rethink the change of the title of the Guidelines and find a naming that retains the globally accepted wording of net neutrality.

Sincerely,

epicenter.works - for digital rights (Austria)
European Digital Rights (Europe)
Article19 (Global)
Access Now (Global)
Homo Digitalis (Greece)
Chaos Computer Club e.V (Germany)
XNet (Spain)
D3 Defesa dos Direitos Digitais (Portugal)
Bits of Freedom (Netherlands)
Open Rights Group (United Kingdom)
La Quadrature du Net (France)

ApTI - Asociația pentru Tehnologie și Internet (Romania)
Digitalcourage e.V. (Germany)
FITUG e.V. (Germany)
IT-Pol - IT-Political Association of Denmark (Denmark)
CitizenD (Slovenia)
Iuridicum Remedium, z.s. (Czech Republic)
Hermes Center (Spain)
Electronic Frontier Norway (Norway)
Electronic Frontier Finland (Finland)
Entropia e.V. CCC Karlsruhe (Germany)
Digitale Gesellschaft e.V (Germany)
Deutsche Vereinigung für Datenschutz e.V. (Germany)