BoR (16) 94

BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules

Background and general aspects

1. These BEREC Guidelines drafted in accordance with Article 5(3) of the Regulation[1] are designed to provide guidance on the implementation of the obligations of NRAs. Specifically, this includes the obligations to closely monitor and ensure compliance with the rules to safeguard equal and non-discriminatory treatment of traffic in the provision of internet access services and related end-users rights as laid down in Articles 3 and 4. These Guidelines constitute recommendations to NRAs, and NRAs should take utmost account of the Guidelines[2]. The Guidelines should contribute to the consistent application of the Regulation, thereby contributing to regulatory certainty for stakeholders.

Terminology

2. For the purpose of these Guidelines, BEREC has used the following terms throughout the Guidelines to improve readability[3].

1 Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2120&from=EN

2 As set out in Article 3(3) of the Regulation (EC) No 1211/2009 establishing the Body of European Regulators of Electronic Communications and the Office, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0001:0010:EN:PDF and recital 19 of Regulation (EU) 2015/2120

3 Definitions of terms used in the Regulation are provided in the relevant parts of the Guidelines

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

Article 1
Subject matter and scope

This Regulation establishes common rules to safeguard equal and non-discriminatory treatment of traffic in the provision of internet access services and related end-users’ rights.

Recital 1

This Regulation aims to establish common rules to safeguard equal and non-discriminatory treatment of traffic in the provision of internet access services and related end-users’ rights. It aims to protect end-users and simultaneously to guarantee the continued functioning of the internet ecosystem as an engine of innovation.

Recital 2

The measures provided for in this Regulation respect the principle of technological neutrality, that is to say they neither impose nor discriminate in favour of the use of a particular type of technology.

Recital 3

The internet has developed over the past decades as an open platform for innovation with low access barriers for end-users, providers of content, applications and services and providers of internet access services. The existing regulatory framework aims to promote the ability of end-users to access and distribute information or run applications and services of their choice. However, a significant number of end-users are affected by traffic management practices which block or slow down specific applications or services. Those tendencies require common rules at the Union level to ensure the openness of the internet and to avoid fragmentation of the internal market resulting from measures adopted by individual Member States.

3. Article 1 sets out the subject matter and scope of the Regulation, which is to establish common rules to safeguard *“equal and non-discriminatory treatment of traffic in the provision of internet access services”* and *“related end-users’ rights”*.

4. According to the Framework Directive[4], *"end-user"* means a user not providing public communications networks or publicly available electronic 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.

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

6. NRAs may take into account the interconnection policies and practices of ISPs in so far as they have the effect of limiting the exercise end-user rights under Article 3(1). For example, this may be relevant in some cases, such as if the interconnection is implemented in a way which seeks to circumvent the Regulation[5].

Article 2
Definitions

For the purposes of this Regulation, the definitions set out in Article 2 of Directive 2002/21/EC apply. The following definitions also apply:

7. The definitions of Article 2 of Directive 2002/21/EC also apply for the purposes of these Guidelines. This includes the terms *"end-user"*, *"consumer"*, *"electronic*

4 Article 2 of Framework Directive (2002/21/EC) ref. lit. (n) and lit. (h). The directive has been amended by the regulation 717/2007/EC, the regulation 544/2009/EC and the directive 2009/140/EC (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0021:20091219:EN:PDF)

5 Recital 7: *"Such agreements, as well as any commercial practices of providers of internet access services, should not limit the exercise of those rights and thus circumvent provisions of this Regulation safeguarding open internet access"*

communications services", "electronic communications network" and *"network termination point (NTP)"*.

"Provider of electronic communications to the public"

(1) 'provider of electronic communications to the public' means an undertaking providing public communications networks or publicly available electronic communications services;

8. The term *"provider of electronic communications to the public"* (PECP) comprises both *"public communications networks"* and *"electronic communications services"* (ECS), which are defined in Article 2 of the Framework Directive.[6]

9. Conversely, the definition of PECP does not cover providers of electronic communication services or communication networks that are *not* publicly available, which are therefore out of scope of this Regulation.

10. Electronic communication services or networks that are offered not only to a predetermined group of end-users but in principle to any customer who wants to subscribe to the service or network should be considered to be publicly available. Electronic communication services or networks that are offered only to a *predetermined* group of end-users could be considered to be not publicly available.

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

6 Ref. Article 2 letter (d) for *"public communications network"* and letter (c) for *"electronic communications service"*

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

12. The following examples could be considered as services or networks not being made publicly available, subject to an assessment of the facts of the case by NRAs as well as national practices:

    - access to the internet provided by cafés and restaurants (e.g. Wi-Fi hotspots), since they typically are limited to customers of an enterprise rather than the general public;
    - Internal corporate networks, since they are typically limited to employees and other people connected with the business or organisation concerned.

"Internet access service"

(2) 'internet access service' means a publicly available electronic communications service that provides access to the internet, and thereby connectivity to virtually all end points of the internet, irrespective of the network technology and terminal equipment used.

Recital 4

An internet access service provides access to the internet, and in principle to all the end-points thereof, irrespective of the network technology and terminal equipment used by end-users. However, for reasons outside the control of providers of internet access services, certain end points of the internet may not always be accessible. Therefore, such providers should be deemed to have complied with their obligations related to the provision of an internet access service within the meaning of this Regulation when that service provides connectivity to virtually all end points of the internet. Providers of internet access services should therefore not restrict connectivity to any accessible end-points of the internet.

13. Article 2(2) defines an *"internet access service"* (IAS) as an ECS that provides access to the internet, and thereby connectivity to virtually all end points of the internet, irrespective of the network technology and terminal equipment used.

14. For the purpose of the Regulation, BEREC understands the term *"internet"* as referring to a global system of interconnected networks that enables connected end-users to connect to one another. An IAS enables such access to the internet.

15. BEREC understands the term *"connectivity to virtually all end-points"* as a consequence of the fact that the internet is a distributed system where a single ISP controls a rather limited part. Due to reasons outside the control of an individual ISP (e.g. technical limitations, the policy of other ISPs or regulation in some countries), not all endpoints might be reachable all of the time. However, such a lack of reachability should not preclude that the service is defined as an IAS.

16. Where restrictions to reach end-points stem from the use of two different internet addressing schemes, IPv4 and IPv6, this typically does not mean the services cannot be defined as an IAS. While it is not possible to connect two different points with different types of addresses without any translation function, BEREC considers that the term *"virtually all end points"* should, at present, not be interpreted as a requirement on ISPs to offer connectivity with both IPv4 and IPv6.

17. BEREC understands a sub-internet service to be an IAS which would restrict access to services or applications (e.g. banning the use of VoIP or video streaming) or would enable access to only a pre-defined part of the internet (e.g. access only to particular websites). NRAs should take into account that an ISP could easily circumvent the application of the Regulation by providing such sub-internet offers. These services should therefore be considered to be in the scope of the Regulation and the fact that such offers provide a limited access to the internet should qualify as an infringement of Articles 3(1), 3(2) and 3(3) of the Regulation. BEREC refers to these service offers as "sub-internet services", as further discussed in paragraph If an ISP contractually (as opposed to technically) banned the use of specific content, or one or more applications/services or categories thereof (for example, banning the use of VoIP) this would limit the exercise of the end-user rights set out in Article 3(1). This would be considered to be an offer of a sub-internet service (see paragraph BEREC understands a sub-internet service to be an IAS which would restrict access to services or applications (e.g. banning the use of VoIP or video streaming) or would enable access to only a pre-defined part of the internet (e.g. access only to particular websites). NRAs should take into account that an ISP could easily circumvent the application of the Regulation by providing such sub-internet offers. These services should therefore be considered to be in the scope of the Regulation and the fact that such offers provide a limited access to the internet should qualify as an infringement of Articles 3(1), 3(2) and 3(3) of the Regulation.). and In case of agreements or practices involving technical discrimination, this would constitute unequal treatment which would not be compatible with Article 3(3). This holds in particular for the following examples:.

18. Applications where the amount of reachable end-points is limited by the nature of the terminal equipment used (everything used beyond the network

termination point) are outside the scope of the Regulation. This includes applications designed for communication with individual devices, such as e-book readers as well as machine-to-machine[7] devices like smart meters etc.). Such applications should not be used to circumvent this Regulation, e.g. by means of other services usable or offered as a replacement for an IAS. The underlying connectivity could be provided using a private network or an IAS or be part of a specialised service where the application and connectivity is bundled. In the latter two cases (IAS and specialised services), the underlying connectivity service should comply with the Regulation.[8]

7 However, some machine-to-machine communication services may also represent a specialised service according to Article 3(5) of the Regulation (ref. Recital 16 and paragraph Typical examples of specialised services provided to end-users are VoLTE and linear broadcasting IPTV services with specific QoS requirements, subject to them meeting the requirements of the Regulation, in particular Article 3(5) first subparagraph. Under the same preconditions, other examples would include real-time health services (e.g. remote surgery) or "some services responding to a public interest or by some new machine-to-machine communications services" (Recital 16). of these Guidelines). Moreover, a provider of an M2M device or M2M service (e.g. car manufacturer, provider of energy including smart meter) typically does not seem to provide an ECS under the present regulatory framework, whereas the connectivity service provider which provides connectivity over a public network for remuneration is generally the provider of an ECS in the IoT value chain, ref. BEREC Report on Enabling the Internet of Things, BoR (16) 39, pages 21-23.

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

Article 3
Safeguarding of open internet access

19. Article 3 comprises measures intended to safeguard open internet access, covering the rights of the end-users of IAS, and obligations and permitted practices for the ISPs:
    - Article 3(1) sets out the rights of end-users of IAS;
    - Article 3(2) sets limits on the contractual conditions which may be applied to IAS and the commercial practices of ISPs providing IAS, and requires that these should not limit exercise of the end-user rights set out in paragraph 1. When assessing commercial practices, Article 3(3) should also be taken into account;
    - Article 3(3) constrains ISPs' traffic management practices, setting a requirement that ISPs should treat all data traffic equally and making provision for the specific circumstances under which ISPs may deviate from this rule;
    - Article 3(4) sets out the conditions under which traffic management measures may entail processing of personal data;
    - Article 3(5) sets out the freedom of ISPs and CAPs to provide specialised services as well as the conditions under which this freedom may be exercised.

Article 3(1)

> End-users shall have the right to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice, irrespective of the end-user's or provider's location or the location, origin or destination of the information, content, application or service, via their internet access service.
> This paragraph is without prejudice to Union law, or national law that complies with Union law, related to the lawfulness of the content, applications or services.

Recital 5

When accessing the internet, end-users should be free to choose between various types of terminal equipment as defined in Commission Directive 2008/63/EC (1). Providers of internet access services 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 6

End-users should have the right to access and distribute information and content, and to use and provide applications and services without discrimination, via their internet access service. The exercise of this right should be without prejudice to Union law, or national law that complies with Union law, regarding the lawfulness of content, applications or services. This Regulation does not seek to regulate the lawfulness of the content, applications or services, nor does it seek to regulate the procedures, requirements and safeguards related thereto. Those matters therefore remain subject to Union law, or national law that complies with Union law.

20. Article 3(1) sets out the end-users' rights with regard to the open internet. The notion of end-user is explained in paragraph According to the Framework Directive4, "end-user" means a user not providing public communications networks or publicly available electronic 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. of these Guidelines.

"Access and distribute information and content"

21. Firstly, end-users have the right to access and distribute information and content. *"Access and distribute"* means that the provisions of this Regulation apply to both sending and receiving data over the IAS. *"Information and content"* is intended to cover any form of data that can be sent or received over the IAS.

"Use and provide applications and services"

22. Secondly, end-users have the right to use and provide applications and services. *"Use and provide"* means that the right applies both to consumption and provision of applications and services. *"Applications and services"* means both applications (including client and server software) as well as services.

"Use terminal equipment of their choice"

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

24. In considering whether end-users may use the terminal equipment of their choice, NRAs should assess whether an ISP provides equipment for its subscribers and restricts the end-users' ability to replace that equipment with their own equipment, i.e. provides *"obligatory equipment"*.

25. Moreover, NRAs should consider whether there is an objective technological necessity for the obligatory equipment to be considered as part of the ISP network. If there is not, and if the choice of terminal equipment is limited, the practice would be in conflict with the Regulation. For example, the practice of restricting tethering[9] 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).

Legislation related to the lawfulness of the content, applications or services

26. Article 3(1) second subparagraph specifies that Union law, and national law that complies with Union law, related to the lawfulness of content, applications or

9 Tethering allows an end-user to share the internet connection of a phone or tablet with other devices such as laptops.

services still applies. The TSM Regulation does not seek to regulate the lawfulness of the content, applications or services (ref. Recital 6).

27. Whereas Article 3(1) second subparagraph contains a clarification with regard to the applicability of such legislation, Article 3(3) letter (a) provides for an exception for ISPs to implement measures going beyond reasonable traffic management measures in order to comply with legislation or measures as specified in that exception.

Article 3(2)

> Agreements between providers of internet access services and end-users on commercial and technical conditions and the characteristics of internet access services such as price, data volumes or speed, and any commercial practices conducted by providers of internet access services, shall not limit the exercise of the rights of end-users laid down in paragraph 1.

Recital 7

In order to exercise their rights to access and distribute information and content and to use and provide applications and services of their choice, end-users should be free to agree with providers of internet access services on tariffs for specific data volumes and speeds of the internet access service. Such agreements, as well as any commercial practices of providers of internet access services, should not limit the exercise of those rights and thus circumvent provisions of this Regulation safeguarding open internet access. National regulatory and other competent authorities 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. To this end, the assessment of agreements and commercial practices should, inter alia, take into account the respective market positions of those providers of internet access services, and of the providers of content, applications and services, that are involved. National regulatory and other competent authorities should be required, as part of their monitoring and enforcement function, to intervene when agreements or commercial practices would result in the undermining of the essence of the end-users' rights.

28. Article 3(2) clarifies that agreements between ISPs and end-users on commercial and technical conditions and the characteristics of IAS such as price, data volumes or speed, and any commercial practices conducted by ISPs are allowed, but shall not limit the exercise of the rights of end-users laid down in Article 3(1).

29. To BEREC's understanding, Article 3(2) contains two relevant aspects:

    - the freedom to conclude agreements between ISPs and end-users relating to commercial and technical conditions as well as characteristics of IAS;
    - the provision that such agreements and commercial practices shall not limit the exercise of the end-users' rights laid down in Article 3(1).

Agreements on commercial and technical conditions and the characteristics of internet access services

30. Agreements refer to contractual relationships between ISPs and end-users that may include, as stated in the Regulation, commercial conditions (such as pricing), technical conditions (such as data volumes and speed) and any characteristics of the IAS. It should be noted that it will often be the case that commercial and technical conditions can be intertwined.

Commercial practices

31. Commercial practices may consist of all relevant aspects of ISPs' commercial behaviour, including unilateral practices of the ISP.[10]

10 NRAs should also consider whether the definition of "commercial practices" in Article 2(d) the Unfair Commercial Practices Directive (UCPD) could also provide guidance in understanding the

Shall not limit the exercise of end-users' rights

32. With regard to characteristics of IAS, agreeing on tariffs for specific data volumes and speeds of the IAS would not represent a limitation of the exercise of the end-users' rights (ref. Recital 7). Moreover, BEREC considers that, as long as the data volume and speed characteristics are applied in an application-agnostic way (applying equally to all applications), end-users' rights are likely to be unaffected by these characteristics and conditions.

33. An ISP may bundle the provision of the IAS with an application. For instance, a mobile operator may offer free access to a music streaming application for a period of time to all new subscribers (as opposed to zero-rating, which is explained in paragraphs A specific commercial practice is called zero-rating. This is where an ISP applies a price of zero to the data traffic associated with a particular application or category of applications (and the data does not count towards any data cap in place on the IAS).There are different types of zero-rating practices which could have different effects on end-users and the open internet, and hence on the end-user rights protected under the Regulation.- When assessing such agreements or commercial practices like zero-rating in relation to Article 3(2), NRAs and other competent authorities should take into account the aim of the Regulation to "safeguard equal and non-discriminatory treatment of traffic" (Article 1) and to "guarantee the continued functioning of the internet ecosystem as an engine of innovation" (Recital 1) as well as Recital 7, which directs NRAs and other competent authorities 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", or which would result in "the undermining of the essence of the end-users' rights".). Where the traffic associated with this application is not subject to any preferential traffic management practice, and is not priced differently than the transmission of the rest of the traffic, such commercial practices are deemed not to limit the exercise of the end-users' rights granted under article 3(1).

34. When assessing agreements or commercial practices, NRAs should also take Article 3(3) into account given that, typically, infringements of Article 3(3) (e.g. technical practices, such as blocking access to applications or types of

---

term, ref. *"any acts, omission, course of conduct or representation, commercial communication, including advertising and marketing, by a trader, directly connected with a promotion, sale or supply of a product"*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:149:0022:0039:EN:PDF. However, it should also be noted that the goal of the UCPD is different from the goal of Regulation 2015/2120 inasmuch as the former mainly addresses commercial practices which are directly connected with a promotion, sale or supply of a product (i.e. mainly advertising and marketing) whereas the latter establishes common rules to safeguard equal and non-discriminatory treatment of traffic in the provision of internet access services and related end-users' rights.

applications) will directly limit the exercise of the end-users' rights, and constitute an infringement of Articles 3(2) and 3(1). Details about this assessment can be found in paragraphs A basic principle of the Regulation relates to traffic management and is the obligation on ISPs to treat all traffic equally when providing IAS.-NRAs should monitor that ISPs properly dimension their network, and take into account the following: .

35. If an ISP contractually (as opposed to technically) banned the use of specific content, or one or more applications/services or categories thereof (for example, banning the use of VoIP) this would limit the exercise of the end-user rights set out in Article 3(1). This would be considered to be an offer of a sub-internet service (see paragraph BEREC understands a sub-internet service to be an IAS which would restrict access to services or applications (e.g. banning the use of VoIP or video streaming) or would enable access to only a pre-defined part of the internet (e.g. access only to particular websites). NRAs should take into account that an ISP could easily circumvent the application of the Regulation by providing such sub-internet offers. These services should therefore be considered to be in the scope of the Regulation and the fact that such offers provide a limited access to the internet should qualify as an infringement of Articles 3(1), 3(2) and 3(3) of the Regulation.).

36. However, some commercial conditions or practices, most obviously those involving price differentiation applied to categories of data traffic, are more likely to influence end-users' exercise of the rights defined in Article 3(1) without necessarily limiting it.

37. A specific commercial practice is called zero-rating. This is where an ISP applies a price of zero to the data traffic associated with a particular application or category of applications (and the data does not count towards any data cap in place on the IAS).There are different types of zero-rating practices which could have different effects on end-users and the open internet, and hence on the end-user rights protected under the Regulation.

38. A zero-rating offer where all applications are blocked (or slowed down) once the data cap is reached except for the zero-rated application(s) would infringe Article 3(3) first (and third) subparagraph (see paragraph In case of agreements or practices involving technical discrimination, this would constitute unequal treatment which would not be compatible with Article 3(3). This holds in particular for the following examples:).

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

40. When assessing such agreements or commercial practices like zero-rating in relation to Article 3(2), NRAs and other competent authorities should take into account the aim of the Regulation to *"safeguard equal and non-discriminatory treatment of traffic"* (Article 1) and to "*guarantee the continued functioning of the internet ecosystem as an engine of innovation*" (Recital 1) as well as Recital 7, which directs NRAs and other competent authorities 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*", or which would result in *"the undermining of the essence of the end-users' rights".*

41. Recital 7 also indicates NRAs and other competent authorities should take into account the *"respective market positions of those providers of internet access services, and of the providers of content, applications and services, that are involved"*.

42. When assessing whether an ISP limits the exercise of rights of end-users, NRAs should consider to what extent the end-users' choice is restricted by the agreed commercial and technical conditions or the commercial practices of the ISP. It is not the case that every factor affecting end-users' choices should be considered to limit the exercise of end-users' rights under Article 3(1). Such restrictions would need to result in choice being materially reduced for this to qualify as a limitation of the exercise of the end-users' rights.

43. In light of the aforementioned considerations, BEREC considers that a comprehensive assessment of such commercial and technical conditions may be required, taking into account in particular:
    - the goals of the Regulation and whether the relevant agreements and/or commercial practices circumvent these general aims;
    - the market positions of the ISPs and CAPs involved: a limitation of the exercise of end-user rights is more likely to arise where an ISP or a CAP has a 'strong' market position (all else being equal) compared to a situation where the ISP or CAP has a 'weak' market position. The market positions should be analysed in line with competition law principles.
    - the effects on consumer and business customer end-user rights, which encompasses an assessment of inter alia:
        - whether there is an effect on the range and diversity of content and applications which consumer end-users may use and, if so, whether the range and diversity of applications which end-users can choose from is reduced in practice;
        - whether the end-user is incentivised to use, for example, certain applications;
        - whether the IAS subscription contains characteristics which materially reduce end-user choice (see in more detail in paragraph In applying such a comprehensive assessment, NRAs and other competent authorities may also take into account the following considerations:).
    - the effects on CAP end-user rights, which encompasses an assessment of, inter alia:
        - whether there is an effect on the range and diversity of content and applications which CAPs provide, and to what extent the range and diversity of applications may not be effectively accessed;

    - whether CAPs are materially discouraged from entering the market or forced to leave the market, or whether there are other material harms to competition in the market concerned (see in more detail in the fourth bullet of paragraph In applying such a comprehensive assessment, NRAs and other competent authorities may also take into account the following considerations: with regard to offers);
    - whether the continued functioning of the internet ecosystem as an engine of innovation is impacted, for example, whether it is the ISP that picks winners and losers, and on the administrative and/or technical barriers for CAPs to enter into agreements with ISPs.
- the scale of the practice and the presence of alternatives: a practice is more likely to limit the exercise of end-user rights in a situation where, for example, many end-users are concerned and/or there are few alternative offers and/or competing ISPs for the end-users to choose from;
- the effect on freedom of expression and media pluralism (ref. Recital 13).

44. Each of these factors may contribute to a material reduction in end-user choice and hence a limitation of the exercise of end-users' rights under Article 3(2). In any specific case, the presence of one or more of these factors may in fact limit the exercise of end-user rights.

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

    - Any agreements or practices which have an effect similar to technical blocking of access (see paragraph In case of agreements or practices involving technical discrimination, this would constitute unequal treatment which would not be compatible with Article 3(3). This holds in particular for the following examples:) are likely to infringe Articles 3(1) and 3(2), given their strong impact on end-user rights.
    - Commercial practices which apply a *higher* price to the data associated with a specific application or class of applications are likely to limit the exercise of end-users' rights because of the potentially strong disincentive created to the use of the application(s) affected, and consequent restriction of choice. Also, the possibility that higher prices may be applied to an application or category of application may discourage the development of new applications.
    - End-users of an IAS whose conditions include a lower (or zero) price for the data associated with a specific application or class of applications will be incentivised to use the zero-rated application or category of applications and not others. Furthermore, the lower the data cap, the stronger such influence is likely to be.
    - Price differentiation between *individual* applications within a category has an impact on competition between providers in that class. It may therefore be more likely to impact the "*continued functioning of the internet ecosystem as an engine of innovation"* and thereby undermine the goals of the Regulation than would price differentiation between *classes* of application.

Article 3(3) first subparagraph

Providers of internet access services shall treat all traffic equally, when providing internet access services, without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used.

Recital 8

When providing internet access services, providers of those services should treat all traffic equally, without discrimination, restriction or interference, independently of its sender or receiver, content, application or service, or terminal equipment. According to general principles of Union law and settled case-law, comparable situations should not be treated differently and different situations should not be treated in the same way unless such treatment is objectively justified.

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

47. As Article 3(3) concerns the equal treatment of all traffic *"when providing internet access service",* the scope of this paragraph excludes IP interconnection practices.

48. In assessing whether an ISP complies with this principle, NRAs should apply a two-step assessment:
    - In a first step, they should assess whether all traffic is treated equally.
    - In a second step, they should assess whether situations are comparable or different and whether there are objective grounds which could justify a different treatment of different situations (under Article 3(3) second subparagraph – see paragraphs 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.-BEREC understands that "categories of traffic" should be clearly distinguished from specialised services. below).

49. Moreover, NRAs should ensure that traffic on an IAS is managed:
    - "without discrimination, restriction or interference";
    - "irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used".

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

51. Endpoint-based congestion control[11] (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.

52. In case of agreements or practices involving technical discrimination, this would constitute unequal treatment which would not be compatible with Article 3(3). This holds in particular for the following examples:
    - A practice where an ISP blocks, slows down, restricts, interferes with, degrades or discriminates access to specific content, one or more applications (or categories thereof), except when justified by reference to the exceptions of Article 3(3) third subparagraph.
    - IAS offers where the access to internet is restricted to a limited set of applications or endpoints by the end-user's ISP (sub-internet service offers) infringe upon Article 3(3) first subparagraph, as such offers entail

11 This should not be confused with network-internal congestion management as described under Article 3(3) letter (c)). IETF, RFC 5783, Congestion Control in the RFC Series

12 See details about terminal equipment under Article 3(1)

13 Active Queue Management, see IETF, RFC 7567

blocking of applications and or discrimination, restriction or interference related to the origin or destination of the information.

- 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.

53. NRAs should apply a comprehensive assessment of compatibility with the Regulation for all those IAS offers which are not as clear as the examples mentioned in paragraph In case of agreements or practices involving technical discrimination, this would constitute unequal treatment which would not be compatible with Article 3(3). This holds in particular for the following examples:.

Article 3(3) second subparagraph

The first subparagraph shall not prevent providers of internet access services from implementing reasonable traffic management measures. In order to be deemed to be reasonable, such measures shall be transparent, non-discriminatory and proportionate, and shall not be based on commercial considerations but on objectively different technical quality of service requirements of specific categories of traffic. Such measures shall not monitor the specific content and shall not be maintained for longer than necessary.

Recital 9

The objective of reasonable traffic management is to contribute to an efficient use of network resources and to an optimisation of overall transmission quality responding to the objectively different technical quality of service requirements of specific categories of traffic, and thus of the content, applications and services transmitted. Reasonable traffic management measures applied by providers of internet access services should be transparent, non-discriminatory and proportionate, and should not be based on commercial considerations. The requirement for traffic management measures to be non-discriminatory does not preclude providers of internet access services from implementing, in order to optimise the overall transmission quality, traffic management measures which differentiate between objectively different categories of traffic. Any such differentiation should, in order to optimise overall quality and user experience, be permitted only on the basis of objectively different technical quality of service requirements (for example, in terms of latency, jitter, packet loss, and bandwidth) of the specific categories of traffic, and not on the basis of commercial considerations. Such differentiating measures should be proportionate in relation to the purpose of overall quality optimisation and should treat equivalent traffic equally. Such measures should not be maintained for longer than necessary.

Recital 10

Reasonable traffic management does not require techniques which monitor the specific content of data traffic transmitted via the internet access service.

Traffic management measures[14]

54. In assessing whether an ISP complies with the principle of equal treatment set out in Article 3(3) first subparagraph, NRAs should take into account whether a measure (which, prima facie, appears to infringe this principle) is a reasonable traffic management measure. The principle of equal treatment of traffic does not prevent ISPs from implementing reasonable traffic management measures in compliance with Article 3(3) second subparagraph.

"Transparent, non-discriminatory and proportionate"

55. In considering whether a traffic management measure is reasonable, NRAs should in a first step assess whether the traffic management measure is transparent, non-discriminatory and proportionate. These terms are legal principles that are already used in every-day regulatory practice when applying EU law and respective national law.

56. Under Article 3(3), NRAs should require ISPs to provide *transparent* information about traffic management practices and the impact of these practices (see also Articles 4 and 5).

57. When considering whether a traffic management measure is non-discriminatory, NRAs should consider the following:
    - The requirement for traffic management measures to be non-discriminatory does not preclude ISPs from implementing - in order to optimise the overall transmission quality and user experience - traffic management measures which differentiate between objectively different categories of traffic (ref. Recital 9 and below paragraphs In assessing whether a traffic management measure is reasonable, NRAs should assess the justification put forward by the ISP. In order to be considered to be reasonable, a traffic management measure has to be based on objectively different technical QoS requirements of specific categories of traffic. Examples for technical QoS requirements are latency, jitter, packet loss, and bandwidth.-ISPs may prioritise network management traffic over the rest of their traffic. Such traffic management practices should be considered as reasonable, providing they are transparent. Indeed, these practices are aimed at properly configuring and securing the network and its equipment by efficiently balancing load, e.g. by reacting as fast as possible in case of congestion, failures, outages, etc.).

14 A definition of traffic management measures can be found on page 18 of the BEREC 2011 Net Neutrality QoS Framework (BoR (11) 53)

- Similar situations in terms of similar technical QoS requirements should receive similar treatment;
- Different situations in terms of objectively different technical QoS requirements can be treated in different ways if such treatment is objectively justified;
- In particular, the mere fact that network traffic is encrypted should not be deemed by NRAs to be an objective justification for different treatment by ISPs.

58. When considering whether a traffic management measure is proportionate, NRAs should consider the following:
    - There has to be a legitimate aim for this measure, as specified in the first sentence of Recital 9, namely contributing to an efficient use of network resources and to an optimisation of overall transmission quality;
    - The traffic management measure has to be suitable to achieve the aim (with a requirement of evidence to show it will have that effect, and that it is not manifestly inappropriate);
    - The traffic management measure has to be necessary to achieve the aim;
    - There is not a less interfering and equally effective alternative way of achieving this aim (e.g. equal treatment without categories of traffic) with the available network resources;
    - The traffic management measure has to be appropriate, e.g. to balance the competing requirements of different traffic categories or competing interests of different groups.

"Objectively different technical QoS requirements of traffic categories"

59. In assessing whether a traffic management measure is reasonable, NRAs should assess the justification put forward by the ISP. In order to be considered to be reasonable, a traffic management measure has to be based on objectively different technical QoS requirements of specific categories of traffic. Examples for technical QoS requirements are latency, jitter, packet loss, and bandwidth.

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 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.[15]

15 IETF, RFC 7657, Differentiated Services and Real-Time Communication

61. Furthermore, as explained in Recital 9, ISPs' traffic management measures are "responding to" the QoS requirements of the categories of traffic in order to optimise the overall transmission quality and enhance the user-experience. In order to identify categories of traffic, the ISP relies on the information provided by the application when packets are sent into the network. (See also paragraph 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 as generic content, as opposed to the specific content provided by end-users themselves (such as text, pictures and video). regarding which information can legitimately be considered by ISPs). Encrypted traffic should not be treated less favourably by reason of its encryption.

62. When NRAs consider network-internal mechanisms of ISPs which assist endpoint-based congestion control (see paragraph Endpoint-based congestion control11 (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 control13 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.) in the context of Article 3(3) second subparagraph, the queue management of the different traffic categories[16] should be assessed under the same criteria as described in general for Article 3(3) second subparagraph.

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

    - that application layer protocol or generic application type are linked to objectively different technical QoS requirements;
    - applications with equivalent QoS requirements are handled agnostically in the same traffic category;

16 See section 2.1 "AQM and Multiple Queues" in IETF RFC 7567

- justifications are specific to the objectives that are pursued by implementing traffic management measures based on different categories of traffic.

64. ISPs may prioritise network management traffic over the rest of their traffic. Such traffic management practices should be considered as reasonable, providing they are transparent. Indeed, these practices are aimed at properly configuring and securing the network and its equipment by efficiently balancing load, e.g. by reacting as fast as possible in case of congestion, failures, outages, etc.

"Not based on commercial considerations"

65. In the event that traffic management measures are based on commercial grounds, the traffic management measure is not reasonable. An obvious example of this could be where an ISP charges for usage of different traffic categories. However, NRAs do not need to prove that a traffic management measure is based on commercial grounds; it is sufficient to establish that the traffic management measure is not based on objectively different technical QoS requirements.

"Shall not monitor the specific content"

66. In assessing traffic management measures, NRAs should ensure that such measures do not monitor the specific content (i.e. transport layer protocol payload).

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 as generic content, as opposed to the specific content provided by end-users themselves (such as text, pictures and video).

"Shall not be maintained longer than necessary"

68. In assessing traffic management measures, NRAs should take into account that such measures shall not be maintained longer than necessary.

69. BEREC understands this term as relating to the proportionality of reasonable traffic management measures in terms of duration, in parallel to the explicit precondition *"shall be proportionate"* which relates to their proportionality in terms of scope (type and proportion of traffic affected, impact on the rest of traffic, equal treatment of comparable situations etc.).

70. This does not prevent, per se, a trigger function to be implemented and in place (but with the traffic management measure not yet effective) on an ongoing basis inasmuch as the traffic management measure only becomes effective in times of necessity. Necessity can materialise several times, or even regularly, over a given period of time. However, where traffic management measures are permanent or recurring, their necessity might be questionable and NRAs should, in such scenarios, consider whether the traffic management measures can still be qualified as reasonable within the meaning of Article 3(3) second subparagraph.

Distinction from exceptional traffic management measures

71. Article 3(3) third subparagraph clarifies that, under Article 3(3) second subparagraph, inter alia the following traffic management measures are prohibited: blocking, slowing down, alteration, restriction, interference with, degradation, and discrimination between specific content, applications or services, or specific categories thereof.

Distinction from specialised services

72. BEREC understands that *"categories of traffic"* should be clearly distinguished from specialised services. Article 3(5) clarifies that specialised services may be provided for optimisation reasons in order to meet requirements for a specific level of quality. On the other hand, any use of *"categories of traffic"* under Article 3(3) second subparagraph is permitted for the optimisation of the overall transmission quality (ref. Recital 9).

Article 3(3) third subparagraph

Providers of internet access services shall not engage in traffic management measures going beyond those set out in the second subparagraph, and in particular shall not block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services, or specific categories thereof, except as necessary, and only for as long as necessary, in order to:

Recital 11

Any traffic management practices which go beyond such reasonable traffic management measures, by blocking, slowing down, altering, restricting, interfering with, degrading or discriminating between specific content, applications or services, or specific categories of content, applications or services, should be prohibited, subject to the justified and defined exceptions laid down in this Regulation. Those exceptions should be subject to strict interpretation and to proportionality requirements. Specific content, applications and services, as well as specific categories thereof, should be protected because of the negative impact on end-user choice and innovation of blocking, or of other restrictive measures not falling within the justified exceptions. Rules against altering content, applications or services refer to a modification of the content of the communication, but do not ban non- discriminatory data compression techniques which reduce the size of a data file without any modification of the content. Such compression enables a more efficient use of scarce resources and serves the end-users' interests by reducing data volumes, increasing speed and enhancing the experience of using the content, applications or services concerned.

Recital 12

Traffic management measures that go beyond such reasonable traffic management measures may only be applied as necessary and for as long as necessary to comply with the three justified exceptions laid down in this Regulation.

73. Article 3(3), third subparagraph contains two aspects:

    - a prohibition for ISPs to apply traffic management measures going beyond reasonable traffic management measures; as well as
    - an exhaustive list of three exceptions in which traffic managements measures that go beyond such reasonable traffic management are permissible.

74. In order to safeguard the open Internet, Article 3(3) third subparagraph describes traffic management practices that are prohibited, unless under specific exception. These are practices that, inter alia, are banned in that regard, and can be described by these seven basic principles which should be used by NRAs when assessing ISPs' practices:

    - no blocking,

- no slowing down,
- no alteration,
- no restriction,
- no interference with,
- no degradation and
- no discrimination

between specific content, applications or services, or specific categories thereof. This is a non-exhaustive list of traffic management measures that are prohibited, and any other measure going beyond reasonable traffic management is also prohibited. Practices not complying with the seven basic principles, or that otherwise go beyond reasonable traffic management, may be used by ISPs only based on the three specific exceptions elaborated below under Article 3(3) letters (a), (b) and (c).

75. 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 network-internal blocking put in place by the ISP, terminal equipment-based restrictions put in place by the end-user are not targeted by the Regulation.
76. The three exceptions set out in Article 3(3) third subparagraph have as common preconditions that the traffic management measure has to be necessary for the achievement of the respective exception (*"except as necessary"*) and that it may be applied *"only for as long as necessary"*. These requirements follow from the principle of proportionality.[17] Moreover, as exceptions, they should be interpreted in a strict manner.[18]
77. The prohibition of monitoring of specific content does not apply to traffic management *going beyond reasonable traffic management* (i.e. traffic management complying with the exceptions in letters (a), (b), or (c)). It should be noted that, according to Article 3(4), any processing of personal data has to be carried out in line with Directive 95/46/EC and Directive 2002/58/EC.

17 See recital 11

18 See recital 11

Article 3(3) letter (a)

(a) comply with Union legislative acts, or national legislation that complies with Union law, to which the provider of internet access services is subject, or with measures that comply with Union law giving effect to such Union legislative acts or national legislation, including with orders by courts or public authorities vested with relevant powers;

Recital 13
First, situations may arise in which providers of internet access services are subject to Union legislative acts, or national legislation that complies with Union law (for example, related to the lawfulness of content, applications or services, or to public safety), including criminal law, requiring, for example, blocking of specific content, applications or services. In addition, situations may arise in which those providers are subject to measures that comply with Union law, implementing or applying Union legislative acts or national legislation, such as measures of general application, court orders, decisions of public authorities vested with relevant powers, or other measures ensuring compliance with such Union legislative acts or national legislation (for example, obligations to comply with court orders or orders by public authorities requiring to block unlawful content). The requirement to comply with Union law relates, inter alia, to the compliance with the requirements of the Charter of Fundamental Rights of the European Union ('the Charter') in relation to limitations on the exercise of fundamental rights and freedoms. As provided in Directive 2002/21/EC of the European Parliament and of the Council (1), any measures liable to restrict those fundamental rights or freedoms are only to be imposed if they are appropriate, proportionate and necessary within a democratic society, and if their implementation is subject to adequate procedural safeguards in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms, including its provisions on effective judicial protection and due process.

78. If an ISP applies traffic management measures which cannot be regarded as reasonable, NRAs should assess whether an ISP does so because it has to do so for legal reasons, namely to comply with the legislation or measures by public authorities specified in that exception.

Article 3(3) letter (b)

(b) preserve the integrity and security of the network, of services provided via that network, and of the terminal equipment of end-users;

Recital 14
Second, traffic management measures going beyond such reasonable traffic management measures might be necessary to protect the integrity and security of the network, for example by preventing cyber-attacks that occur through the spread of malicious software or identity theft of end-users that occurs as a result of spyware.

79. Typical attacks and threats that will trigger integrity and security measures include:
    - flooding network components or terminal equipment with traffic to destabilise them (e.g. Denial of Service attack);
    - spoofing IP addresses in order to mimic network devices or allow for unauthorised communication;
    - hacking attacks against network components or terminal equipment;
    - distribution of malicious software, viruses etc.
80. Conducting traffic management measures in order to preserve integrity and security of the network could basically consist of restricting connectivity or blocking of traffic to and from specific endpoints. Typical examples of such traffic management measures include:
    - blocking of IP addresses, or ranges of them, because they are well-known sources of attacks;

- blocking of IP addresses from which an actual attack is originating;
- blocking of IP addresses/IAS showing suspicious behaviour (e.g. unauthorised communication with network components, address spoofing);
- blocking of IP addresses where there are clear indications that they are part of a bot network;
- blocking of specific port numbers which constitute a threat to security and integrity.

81. NRAs should consider that, in order to identify attacks and activate security measures, the use of security monitoring systems by ISPs is often justified. In such cases, the monitoring of traffic to detect security threats, such as those listed in paragraph Conducting traffic management measures in order to preserve integrity and security of the network could basically consist of restricting connectivity or blocking of traffic to and from specific endpoints. Typical examples of such traffic management measures include:) may be implemented in the background, while the actual traffic management measure preserving integrity and security is triggered only when security attacks are detected. Therefore, the precondition *"only for as long as necessary"* does not preclude implementation of such monitoring of the integrity and security of the network.
82. Besides monitoring the integrity and security of the network, possible security threats may also be identified on the basis of reports/complaints from end-users or blocking lists from recognised security organisations.
83. This exception could be used as a basis for circumvention of the Regulation because security is a broad concept. NRAs should therefore carefully assess whether the requirements of this exception are met and to request that ISPs provide adequate justifications when necessary.

Article 3(3) letter (c)

(c) prevent impending network congestion and mitigate the effects of exceptional or temporary network congestion, provided that equivalent categories of traffic are treated equally.

Recital 15
Third, measures going beyond such reasonable traffic management measures might also be necessary to prevent impending network congestion, that is, situations where congestion is about to materialise, and to mitigate the effects of network congestion, where such congestion occurs only temporarily or in exceptional circumstances. The principle of proportionality requires that traffic management measures based on that exception treat equivalent categories of traffic equally. Temporary congestion should be understood as referring to specific situations of short duration, where a sudden increase in the number of users in addition to the regular users, or a sudden increase in demand for specific content, applications or services, may overflow the transmission capacity of some elements of the network and make the rest of the network less reactive. Temporary congestion might occur especially in mobile networks, which are subject to more variable conditions, such as physical obstructions, lower indoor coverage, or a variable number of active users with changing location. While it may be predictable that such temporary congestion might occur from time to time at certain points in the network – such that it cannot be regarded as exceptional – it might not recur so often or for such extensive periods that a capacity expansion would be economically justified. Exceptional congestion should be understood as referring to unpredictable and unavoidable situations of congestion, both in mobile and fixed networks. Possible causes of those situations include a technical failure such as a service outage due to broken cables or other infrastructure

elements, unexpected changes in routing of traffic or large increases in network traffic due to emergency or other situations beyond the control of providers of internet access services. Such congestion problems are likely to be infrequent but may be severe, and are not necessarily of short duration. The need to apply traffic management measures going beyond the reasonable traffic management measures in order to prevent or mitigate the effects of temporary or exceptional network congestion should not give providers of internet access services the possibility to circumvent the general prohibition on blocking, slowing down, altering, restricting, interfering with, degrading or discriminating between specific content, applications or services, or specific categories thereof. Recurrent and more long-lasting network congestion which is neither exceptional nor temporary should not benefit from that exception but should rather be tackled through expansion of network capacity.

84. In exceptional cases, and for no longer than necessary, ISPs may engage in traffic management beyond the limits of Article 3(3) second subparagraph to manage certain types of network congestion, namely impending network congestions (which may be prevented) and exceptional or temporary network congestions (the effects of which may be mitigated). Recital 15 provides detailed information on identifying situations where exceptional and temporary congestion occurs. Impending network congestion is defined as situations where congestion is about to materialise, i.e. it is imminent.

85. Recital 15 focuses on exceptional and temporary network congestion; thus, actions for preventing impending network congestion only apply to cases of such congestion.

86. When assessing congestion management exceptions under letter (c), NRAs should refer to the general criteria of strict interpretation and proportionality set out in Article 3(3) third subparagraph. Furthermore, NRAs should check that congestion management is not used to circumvent the ban on blocking, throttling and discrimination, (ref. Recital 15).

87. Due to the requirement that exceptional traffic management can only be applied as necessary, and only for as long as necessary, NRAs should consider that in cases when application-agnostic congestion management (i.e. congestion management which is not targeting specific applications or categories thereof) is not sufficient, congestion can be dealt with according to Article 3(3) letter (c). Furthermore, in such cases equivalent categories of traffic must be treated equally. Any throttling action should be limited to the section of the network where congestion occurs, if feasible.

88. Congestion management can be done on a general basis, independent of applications.[19] NRAs should consider whether such types of congestion

19 IETF, RFC 6057, Comcast's Protocol-Agnostic Congestion Management and IETF, RFC 6789, Congestion Exposure (Conex) Concepts and Use Cases

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 *throttling* of traffic, as opposed to *blocking* of traffic, would be sufficient and equally effective to manage congestion.

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

    - if there is recurrent and more long-lasting network congestion in an ISP's network, the ISP cannot invoke the exception of congestion management (ref. Recital 15);
    - application-specific congestion management should not be applied or accepted as a substitute for more structural solutions, such as expansion of network capacity.

Article 3(4)

> Any traffic management measure may entail processing of personal data only if such processing is necessary and proportionate to achieve the objectives set out in paragraph 3. Such processing shall be carried out in accordance with Directive 95/46/EC of the European Parliament and of the Council. Traffic management measures shall also comply with Directive 2002/58/EC of the European Parliament and of the Council.

90. In the course of traffic management, personal data may be processed. Article 3(4) provides that such measures may only process of personal data if certain requirements are met, and only under certain conditions.

91. Article 3(3) distinguishes between reasonable traffic management measures and traffic management measures going beyond reasonable traffic management measures. Article 3(4) applies to both of these traffic management forms *("any traffic management measure"*). With regard to reasonable traffic management measures, these requirements are further specified by Article 3(3) second subparagraph which states *"such measures shall not monitor the specific content"*.

92. The objectives referred to in Article 3(4) are those set out in Article 3(3).

"Necessary and proportionate"

93. The processing of personal data within the course of traffic management is also subject to the proportionality requirement. NRAs should assess whether the processing of personal data undertaken by ISPs is necessary and proportionate to achieve the objectives set out in Article 3(3).

"Compliance with Union law on data protection"

94. NRAs should assess whether the processing of personal data complies with Union law on data protection.[20]

---

20 Whereas NRAs are not competent to enforce the Privacy Directive (Directive 95/46/EC as amended by Regulation (EC) 1882/2003 (http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:l14012&from=EN) they are in many countries empowered to enforce the ePrivacy Directive (Directive 2002/58/EC, as amended by Directive 2006/24/EC and Directive 2009/136/EC (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:PDF)

Article 3(5) first subparagraph

Providers of electronic communications to the public, including providers of internet access services, and providers of content, applications and services shall be free to offer services other than internet access services which are optimised for specific content, applications or services, or a combination thereof, where the optimisation is necessary in order to meet requirements of the content, applications or services for a specific level of quality.

Recital 16

There is demand on the part of providers of content, applications and services to be able to provide electronic communication services other than internet access services, for which specific levels of quality, that are not assured by internet access services, are necessary. Such specific levels of quality are, for instance, required by some services responding to a public interest or by some new machine-to-machine communications services. Providers of electronic communications to the public, including providers of internet access services, and providers of content, applications and services should therefore be free to offer services which are not internet access services and which are optimised for specific content, applications or services, or a combination thereof, where the optimisation is necessary in order to meet the requirements of the content, applications or services for a specific level of quality. 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, applications or services and to enable a corresponding quality assurance to be given to end-users, rather than simply granting general priority over comparable content, applications or services available via the internet access service and thereby circumventing the provisions regarding traffic management measures applicable to the internet access services.

95. Beyond the delivery of a relatively high quality application through the IAS, there can be demand for a category of electronic communication services that need to be carried at a specific level of quality that cannot be assured by the standard best effort delivery.
96. Such services can be offered by providers of electronic communications to the public (PECPs), including providers of internet access services (ISPs), and providers of content, applications and services (CAPs).
97. These providers are free to offer services referred to in Article 3(5), which BEREC refers to as specialised services, only when various requirements are met. Article 3(5) provides the safeguards for the provisioning of specialised services which are characterised by the following features in Article 3 (5) first subparagraph:
    - they are services other than IAS services;
    - they are optimised for specific content, applications or services, or a combination thereof;
    - the optimisation is objectively necessary in order to meet requirements for a specific level of quality.
98. Their provision is subject to a number of conditions in Article 3(5) second subparagraph, namely that:
    - the network capacity is sufficient to provide the specialised service in addition to any IAS provided;
    - specialised services are not usable or offered as a replacement for IAS;
    - specialised services are not to the detriment of the availability or general quality of the IAS for end-users.

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

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

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

Assessment according to Article 3(5) first subparagraph

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

103. When assessing whether the practices used to provide specialised services comply with Article 3(5) first subparagraph, NRAs should apply the approach set out in paragraphs NRAs could request from the provider relevant information about their specialised services, using powers conferred by Article 5(2). In their responses, the provider should give information about their specialised services, including what the relevant QoS requirements are, e.g. latency, jitter and packet loss, including any contractual requirements. Furthermore, the “specific level of quality” should be specified, and it should be demonstrated that this specific

level of quality cannot be assured over the IAS.-Business customers often request services relating to virtual private networks (VPN), which are also discussed in paragraph Regarding virtual private networks (VPN) network services, these are typically provided by the ISP to anyone that wishes to enter a contract about the provision of such a service, and these would therefore typically be considered to be publicly available. The term 'private' describes the use of such a service which is usually limited to endpoints of the business entering the contract and secured for internal communications. In accordance with Recital 17, to the extent that VPNs provide access to the internet, they are not a closed user group and should therefore be considered as publicly available ECS and are subject to Articles 3(1)-(4). VPNs are further discussed in paragraph Business customers often request services relating to virtual private networks (VPN), which are also discussed in paragraph Regarding virtual private networks (VPN) network services, these are typically provided by the ISP to anyone that wishes to enter a contract about the provision of such a service, and these would therefore typically be considered to be publicly available. The term 'private' describes the use of such a service which is usually limited to endpoints of the business entering the contract and secured for internal communications. In accordance with Recital 17, to the extent that VPNs provide access to the internet, they are not a closed user group and should therefore be considered as publicly available ECS and are subject to Articles 3(1)-(4). VPNs are further discussed in paragraph Business customers often request services relating to virtual private networks (VPN), which are also discussed in paragraph Regarding virtual private networks (VPN) network services, these are typically provided by the ISP to anyone that wishes to enter a contract about the provision of such a service, and these would therefore typically be considered to be publicly available. The term 'private' describes the use of such a service which is usually limited to endpoints of the business entering the contract and secured for internal communications. In accordance with Recital 17, to the extent that VPNs provide access to the internet, they are not a closed user group and should therefore be considered as publicly available ECS and are subject to Articles 3(1)-(4). VPNs are further discussed in paragraph Business customers often request services relating to virtual private networks (VPN), which are also discussed in paragraph 11 above. The term VPN can be used in relation to two different types of services:. above. The term VPN can be used in relation to two different types of services:. above. The term VPN can be used in relation to two different types of services:. above. The term VPN can be used in relation to two different types of services:).

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

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

106. If assurance of a specific level of quality is objectively necessary this cannot be provided by simply granting general priority over comparable content.[21] 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.

107. NRAs should verify whether, and to what extent, optimised delivery is objectively necessary to ensure one or more specific and key features of the applications, and to enable a corresponding quality assurance to be given to end-users. To do this, the NRA should assess whether an electronic communication service, other than IAS, requires a level of quality that cannot be assured over an IAS. If not, these electronic communication services are likely to circumvent the provisions of the Regulation and are therefore not allowed.

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

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

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

---

21 As explained in Recital 16, NRAs *"should verify whether and to what extent such optimisation is objectively necessary to ensure one or more specific and key features of the content, applications or services and to enable a corresponding quality assurance to be given to end-users, rather than simply granting general priority over comparable content, applications or services available via the internet access service and thereby circumventing the provisions regarding traffic management measures applicable to the internet access services"*

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

- “VPN application”: A VPN application is typically used in the context of teleworking. A computer (e.g. an employee’s laptop) uses the public internet to connect to corporate services. In order to protect the information transferred, a VPN application on the client encrypts all traffic and typically sends all traffic to a VPN concentrator located within the corporate network. Both ends - the client and the concentrator - use an IAS, and this would therefore not be a specialised service.
- “VPN network service”: A VPN network service is typically used to provide a private connection between a number of sites (e.g. different locations of a corporation). Such VPN services are typically implemented over common infrastructure with IAS (e.g. based on MPLS[22]). Such services are provided

22

in parallel with IAS. As long as the services comply with the requirements set out in the Regulation, they are considered to be specialised services.

Article 3(5) second subparagraph

> Providers of electronic communications to the public, including providers of internet access services, may offer or facilitate such services only if the network capacity is sufficient to provide them in addition to any internet access services provided. Such services shall not be usable or offered as a replacement for internet access services, and shall not be to the detriment of the availability or general quality of internet access services for end-users.

Recital 17

In order to avoid the provision of such other services having a negative impact on the availability or general quality of internet access services for end-users, sufficient capacity needs to be ensured. Providers of electronic communications to the public, including providers of internet access services, should, therefore, offer such other services, or conclude corresponding agreements with providers of content, applications or services facilitating such other services, only if the network capacity is sufficient for their provision in addition to any internet access services provided. The provisions of this Regulation on the safeguarding of open internet access should not be circumvented by means of other services usable or offered as a replacement for internet access services. However, 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 a replacement of the internet access services, provided that the provision of such access to the internet by a provider of electronic communications to the public complies with Article 3(1) to (4) of this Regulation, and therefore cannot be considered to be a circumvention of those provisions. The provision of such services other than internet access services should not be to the detriment of the availability and general quality of internet access services for end-users. In mobile networks, traffic volumes in a given radio cell are more difficult to anticipate due to the varying number of active end-users, and for this reason an impact on the quality of internet access services for end-users might occur in unforeseeable circumstances. In mobile networks, the general quality of internet access services for end-users should not be deemed to incur a detriment where the aggregate negative impact of services other than internet access services is unavoidable, minimal and limited to a short duration. National regulatory authorities should ensure that providers of electronic communications to the public comply with that requirement. In this respect, national regulatory authorities should assess the impact on the availability and general quality of internet access services by analysing, inter alia, quality of service parameters (such as latency, jitter, packet loss), the levels and effects of congestion in the network, actual versus advertised speeds, the performance of internet access services as compared with services other than internet access services, and quality as perceived by end-users.

Sufficient network capacity for specialised services in addition to IAS

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

113. In a network with limited capacity, IAS and specialised services could compete for overall network resources. In order to safeguard the availability of general quality of IAS, the Regulation does not allow specialised services if the network capacity is not sufficient to provide them in addition to any IAS provided,

Multiprotocol Label Switching

because this would lead to degradation of the IAS and thereby circumvent the Regulation. It is the general quality of the IAS which is protected from degradation by the Regulation, rather than specialised services.

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

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

116. NRAs should assess whether or not there is sufficient capacity for IAS when specialised services are provided, for example, by performing measurements of IAS.[23] Methodologies for such measurements have been relatively well developed during BEREC's Net Neutrality QoS workstreams in recent years and will continue to be improved.

Not to the detriment of the availability or general quality of IAS

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

118. While IAS and specialised services directly compete for the dedicated part of a user's capacity the user may determine himself how to use it. Therefore, NRAs should not consider this an infringement of Article 3(5) second subparagraph, as long as the end-user is informed pursuant to Article 4(1)(c) of the likely or

23

See paragraphs IAS performance assessment can be performed at the user or market level:-Market-level assessment data can also be used for:

possible impact on his IAS and can still obtain a minimum speed[24] for any IAS subscribed to in parallel. NRAs should not consider it to be to the detriment of the general quality of ~~IAS when~~IAS when activation of the specialised service by the individual end-user only affects his own IAS. However, detrimental effects should not occur in those parts of the network where capacity is shared between different end-users.

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

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

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

"Not be usable or offered as a replacement for IAS"

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

123. In deciding whether a specialised service is considered as a replacement for an IAS, one important aspect that NRAs should assess is whether the service is actually providing access to the internet but in a restricted way, at a higher

24 As discussed in Article 4(1)(d)

quality, or with differentiated traffic management. If so, this would be considered a circumvention of the Regulation.

Article 4
Transparency measures for ensuring open internet access

Article 4(1)

> Providers of internet access services shall ensure that any contract which includes internet access services specifies at least the following:
>
> *[…letters (a) – (b) – (c) – (d) – (e)…]*
>
> Providers of internet access services shall publish the information referred to in the first subparagraph.

Recital 18

The provisions on safeguarding of open internet access should be complemented by effective end-user provisions which address issues particularly linked to internet access services and enable end-users to make informed choices. Those provisions should apply in addition to the applicable provisions of Directive 2002/22/EC of the European Parliament and of the Council (1) and Member States should have the possibility to maintain or adopt more far- reaching measures. Providers of internet access services should inform end-users in a clear manner how traffic management practices deployed might have an impact on the quality of internet access services, end-users' privacy and the protection of personal data as well as about the possible impact of services other than internet access services to which they subscribe, on the quality and availability of their respective internet access services. In order to empower end-users in such situations, providers of internet access services should therefore inform end-users in the contract of the speed which they are able realistically to deliver. The normally available speed is understood to be the speed that an end-user could expect to receive most of the time when accessing the service. Providers of internet access services should also inform consumers of available remedies in accordance with national law in the event of non-compliance of performance. Any significant and continuous or regularly recurring difference, where established by a monitoring mechanism certified by the national regulatory authority, between the actual performance of the service and the performance indicated in the contract should be deemed to constitute non- conformity of performance for the purposes of determining the remedies available to the consumer in accordance with national law. The methodology should be established in the guidelines of the Body of European Regulators for Electronic Communications (BEREC) and reviewed and updated as necessary to reflect technology and infrastructure evolution. National regulatory authorities should enforce compliance with the rules in this Regulation on transparency measures for ensuring open internet access.

124. NRAs should ensure that ISPs include relevant information referred to in Article 4(1) points (a) to (e) in a clear, comprehensible and comprehensive manner in in contracts that include IAS, and publish that information, for example on an ISP's website.

125. NRAs should also note that the transparency requirements laid down in Articles 4(1) and 4(2) are in addition to the measures provided in directive 2002/22/EC (the Universal Service Directive), particularly in Chapter IV thereof. National law may also lay down additional monitoring, information and transparency requirements, including those concerning the content, form and manner of the information to be published.

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

- should be easily accessible and identifiable for what it is;
- should be accurate and up to date;

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

127. NRAs should ensure that ISPs include in the contract and publish the information elements below, preferably presented in two parts (levels of detail)[25]:
    - The first part should provide high-level (general) information. The information about the IAS provided should include, for example, an explanation of speeds, examples of popular applications that can be used with a sufficient quality, and an explanation of how such applications are influenced by the limitations of the provided IAS. This part should include reference to the second part where the information required by Article 4(1) of the Regulation is provided in more detail.
    - The second part would consist of more detailed technical parameters and their values and other relevant information defined in Article 4(1) of the Regulation and in these Guidelines.
128. Examples of how information could be disclosed in a transparent way can be found in BEREC's 2011 Net Neutrality Transparency Guidelines[26].
129. Contract terms that would inappropriately exclude or limit the exercise of the legal rights of the end-user vis-à-vis the ISP in the event of total or partial non-

25 NRAs should note that ISPs are also under an obligation to provide information to consumers before being bound by the contract under other EU instruments: the Consumer Rights Directive (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0083&rid=1), the Unfair Commercial Practices Directive (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:149:0022:0039:EN:PDF) and the e-Commerce Directive (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN)

26 BEREC Guidelines on Transparency in the scope of Net Neutrality, BoR (11) 67), http://berec.europa.eu/doc/berec/bor/bor11_67_transparencyguide.pdf

performance or inadequate performance by the ISP of any of the contractual obligations might be deemed unfair under national legislation, including the implementation of Directive 93/13/EEC on unfair terms in consumer contracts.[27]

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

Article 4(1) letter (a)

(a) information on how traffic management measures applied by that provider could impact on the quality of the internet access services, on the privacy of end-users and on the protection of their personal data;

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

- how the measures might affect end-user experience in general respect and with regard to specific applications (e.g. where specific categories of traffic are treated differently in accordance with Article 3). Practical examples should be used for this purpose;
- the circumstances and manner under which traffic management measures possibly having an impact as foreseen in Article 4(1) letter (a) are applied[28];

27 See Annex, paragraph 1(b) of Council Directive 93/13/EEC on unfair terms in consumer contracts, (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31993L0013:en:HTML). NRAs may or may not be empowered to monitor compliance with said directive.

28 The Universal Service Directive (Directive 2002/22/EC, Article 20(1)(b) 2nd and 4th indents) may also require such information to be specified in contracts. Article 20(1)(b) 2nd indent requires that contracts specify information on conditions limiting access to and/or use of services and applications, where such conditions are permitted under national law in accordance with Community law

- any measures applied when managing traffic which use 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.

132. The information should be concise and comprehensive. The information should not simply consist of a general condition stating possible impacts of traffic management techniques that could be applied in accordance with the Regulation. Information should also include, at least, a description of the possible impacts of traffic management practices which are in place on the IAS.

133. Modifications to contracts are subject to national legislation implementing Article 20(2) of the Universal Service Directive.

Article 4(1) letter (b)

> (b) a clear and comprehensible explanation as to how any volume limitation, speed and other quality of service parameters may in practice have an impact on internet access services, and in particular on the use of content, applications and services;

134. Besides speed, the most important QoS parameters are delay, delay variation (jitter) and packet loss. These other QoS parameters should be described if they might, in practice, have an impact on the IAS and use of applications. NRAs should ensure that ISPs provide information which is effects-based. Users should be able to understand the implications of these parameters to the usage of applications and whether certain applications (e.g. interactive speech/video or 4K video streaming) cannot in fact be used due to the long delay or slow speed of the IAS. Categories of applications or popular examples of these affected applications could be provided.

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

Article 4(1) letter (c)

> (c) a clear and comprehensible explanation of how any services referred to in Article 3(5) to which the end-user subscribes might in practice have an impact on the internet access services provided to that end-user;

136. NRAs should ensure that ISPs include in the contract and publish clear and comprehensible information about how specialised services included in the end-user's subscription might impact the IAS.

Article 4(1) letter (d)

> (d) a clear and comprehensible explanation of the minimum, normally available, maximum and advertised download and upload speed of the internet access services in the case of fixed networks, or of the estimated maximum and advertised download and upload speed

of the internet access services in the case of mobile networks, and how significant deviations from the respective advertised download and upload speeds could impact the exercise of the end-users' rights laid down in Article 3(1);

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

138. In order for the contractual speed values to be understandable, contracts should specify factors that may have an effect on the speed, both within and outside the ISP's control.

139. BEREC understands that the requirement on ISPs to include in the contract and publish information about *advertised speeds* does not entail a requirement to advertise speeds; rather, it is limited to including in the contract and publishing information about speeds which are advertised by the ISP. The requirement to specify the advertised speed requires an ISP to explain the advertised speed of the particular IAS offer included in the contract, if its speed has been advertised. An ISP may naturally also advertise other IAS offers of higher or lower speeds that are not included in the contract to which the subscriber is party (whether by choice or due to unavailability of the service at their location), in accordance with laws governing marketing.

Specifying speeds for an IAS in case of fixed networks

Minimum speed

140. The minimum speed is the lowest speed that the ISP undertakes to deliver to the end-user, according to the contract which includes the IAS. In principle, the actual speed should not be lower than the minimum speed at any time, except in cases of interruption of the IAS. If the actual speed of an IAS is significantly, and continuously or regularly, lower than the minimum speed, it would indicate non-conformity of performance regarding the agreed minimum speed.

141. NRAs[29] could set requirements on defining minimum speed under Article 5(1), for example that the minimum speed could be in reasonable proportion to the maximum speed.

29 National regulatory authority as referred to in Article 2(g) of the Framework Directive means the body or bodies charged by national law with any of the regulatory tasks assigned in the framework for electronic communications

Maximum speed

142. The maximum speed should be actually achievable by the end-user at least some of the time (e.g. at least once a day). An ISP is not required to technically limit the speed to the maximum speed defined in the contract.

143. NRAs could set requirements on defining maximum speeds under Article 5(1), for example that they are achievable a specified number of times during a specified period.

Normally available speed

144. The normally available speed is the speed that an end-user could expect to receive most of the time when accessing the service. BEREC considers that the normally available speed has two dimensions: the numerical value of the speed and the availability (as a percentage) of the speed during a specified period, such as peak hours or the whole day.

145. The normally available speed should be available during the specified daily period. NRAs could set requirements on defining normally available speeds under Article 5(1), Examples include:

- specifying that normally available speeds should be available at least during off-peak hours and 90% of time over peak hours, or 95% over the whole day;
- requiring that the normally available speed should be in reasonable proportion to the maximum speed.

146. In order to be meaningful, it should be possible for the end-user to evaluate the value of the normally available speed vis-à-vis the actual performance of the IAS on the basis of the information provided.

Advertised speed

147. Advertised speed is the speed an ISP uses in its commercial communications, including advertising and marketing, in connection with the promotion of IAS offers. In the event that speeds are included in an ISP's marketing of an offer (see also paragraph BEREC understands that the requirement on ISPs to include in the contract and publish information about advertised speeds does not entail a requirement to advertise speeds; rather, it is limited to including in the contract and publishing information about speeds which are advertised by the ISP. The requirement to specify the advertised speed requires an ISP to explain the advertised speed of the particular IAS offer included in the contract, if its speed has been advertised. An ISP may naturally also advertise other IAS offers of higher or lower speeds that are not included in the contract to which the subscriber is party (whether by choice or due to unavailability of the service at their location), in accordance with laws governing marketing), the advertised speed should be specified in the published information and in the contract for each IAS offer.

148. NRAs could set requirements on defining advertised speeds under Article 5(1), for example that the advertised speed should not exceed the maximum speed defined in the contract,

Specifying speeds of an IAS in mobile networks

149. Estimated maximum and advertised download and upload speeds should be described in contracts according to paragraphs The estimated maximum speed for a mobile IAS should be specified so that the end-user can understand the realistically achievable maximum speed for their subscription in different locations in realistic usage conditions. The estimated maximum speed could be specified separately for different network technologies that affect the maximum speed available for an end-user. End-users should be able to understand that they may not be able to reach the maximum speed if their mobile terminal does not support the speed.-NRAs could set requirements on defining estimated maximum speeds under Article 5(1), for example that the advertised speed for an IAS as specified in a contract should not exceed the estimated maximum speed as defined in the same contract. See also paragraph BEREC understands that the requirement on ISPs to include in the contract and publish information about advertised speeds does not entail a requirement to advertise speeds; rather, it is limited to including in the contract and publishing information about speeds which are advertised by the ISP. The requirement to specify the advertised speed requires an ISP to explain the advertised speed of the particular IAS offer included in the contract, if its speed has been advertised. An ISP may naturally also advertise other IAS offers of higher or lower speeds that are not included in the contract to which the subscriber is party (whether by choice or due to unavailability of the service at their location), in accordance with laws governing marketing..

Estimated maximum speed

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

151. NRAs could set requirements on defining estimated maximum speeds under Article 5(1).

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

Advertised speed

153. The advertised speed for a mobile IAS offer should reflect the speed which the ISP is realistically able to deliver to end-users. Although the transparency requirements regarding IAS speed are less detailed for mobile IAS than for fixed IAS, the advertised speed should enable end-users to make informed choices, for example, so they are able to evaluate the value of the advertised speed vis-à-vis the actual performance of the IAS. Significant factors that limit the speeds achieved by end-users should be specified.

154. NRAs could set requirements on defining estimated maximum speeds under Article 5(1), for example that the advertised speed for an IAS as specified in a

contract should not exceed the estimated maximum speed as defined in the same contract. See also paragraph BEREC understands that the requirement on ISPs to include in the contract and publish information about advertised speeds does not entail a requirement to advertise speeds; rather, it is limited to including in the contract and publishing information about speeds which are advertised by the ISP. The requirement to specify the advertised speed requires an ISP to explain the advertised speed of the particular IAS offer included in the contract, if its speed has been advertised. An ISP may naturally also advertise other IAS offers of higher or lower speeds that are not included in the contract to which the subscriber is party (whether by choice or due to unavailability of the service at their location), in accordance with laws governing marketing.

Article 4(1) letter (e)

> (e) a clear and comprehensible explanation of the remedies available to the consumer in accordance with national law in the event of any continuous or regularly recurring discrepancy between the actual performance of the internet access service regarding speed or other quality of service parameters and the performance indicated in accordance with points (a) to (d).

155. Remedies available to consumers as described in Article 4(1) letter (e) are defined in national law. Examples of possible remedies for a discrepancy are price reduction, early termination of the contract, damages, or rectification of the non-conformity of performance, or a combination thereof. NRAs should ensure that ISPs provide consumers with information specifying such remedies.

Article 4(2)

> Providers of internet access services shall put in place transparent, simple and efficient procedures to address complaints of end-users relating to the rights and obligations laid down in Article 3 and paragraph 1 of this Article.

156. NRAs should ensure that ISPs adhere to certain good practices regarding procedures for addressing complaints, such as:
    - informing end-users in the contract as well as on their website, in a clear manner, regarding the procedures put in place, including the usual or maximum time it takes to handle a complaint;
    - providing a description of how the complaint will be handled, including what steps the ISP will take to investigate the complaint and how the end-user will be notified of the progress or resolution of the complaint;
    - enabling end-users to easily file a complaint using different means, at least online (e.g. a web-form or email) and at the point of sale, but possibly also using other means such as the post or telephone;
    - providing a single point of contact for all complaints related to the provisions set out in Article 3 and Article 4(1), regardless of the topic of the complaint;
    - enabling an end-user to be able to enquire about the status of their complaint in the same manner in which the complaint was raised;
    - informing end-users of the result of the complaint in a relatively short time, taking into account the complexity of the issue;

- informing the end-user of the means to settle unresolved disputes according to national law if the end-user believes a complaint has not been successfully handled by the ISP (depending upon the cause of the complaint, the competent authority or authorities under national law may be the NRA, a court or an alternative dispute resolution entity etc.).

Article 4(3)

> The requirements laid down in paragraphs 1 and 2 are in addition to those provided for in Directive 2002/22/EC and shall not prevent Member States from maintaining or introducing additional monitoring, information and transparency requirements, including those concerning the content, form and manner of the information to be published. Those requirements shall comply with this Regulation and the relevant provisions of Directives 2002/21/EC and 2002/22/EC.

157. This provision is aimed at Member States and no guidance to NRAs is required.

Article 4(4)

> Any significant discrepancy, continuous or regularly recurring, between the actual performance of the internet access service regarding speed or other quality of service parameters and the performance indicated by the provider of internet access services in accordance with points (a) to (d) of paragraph 1 shall, where the relevant facts are established by a monitoring mechanism certified by the national regulatory authority, be deemed to constitute non-conformity of performance for the purposes of triggering the remedies available to the consumer in accordance with national law.
> This paragraph shall apply only to contracts concluded or renewed from 29 November 2015.

158. The relevant facts proving a significant discrepancy may be established by any monitoring mechanism certified by the NRA, whether operated by the NRA or a third party. The Regulation does not require Member States or an NRA to establish or certify a monitoring mechanism. The Regulation does not define how the certification must be done. If the NRA provides a monitoring mechanism implemented for this purpose it should be considered as a certified monitoring mechanism according to Article 4(4).

159. It would help make the rights enshrined in the Regulation more effective if NRAs were to establish or certify one or more monitoring mechanisms that allow end-users to determine whether there is non-conformity of performance and to obtain related measurement results for use in proving non-conformity of performance of their IAS. The use of any certified mechanism should not be subject to additional costs to the end-user and should be accessible also to disabled end-users.

160. The methodologies that could be used by certified monitoring mechanisms are further discussed in the next section on *Methodology for monitoring IAS performance*. The purpose of this guidance regarding methodologies is to contribute to the consistent application of the Regulation. However, NRAs should be able to use their existing measurement tools and these Guidelines do not require NRAs to change them.

Methodology for monitoring IAS performance

161. NRAs should consider BoR (14) 117[30] when implementing a measurement methodology. Measurements should mitigate, to the extent possible, confounding factors which are internal to the user environment, such as existing cross-traffic and wireless/wireline interface.

162. When implementing measurement methodologies, NRAs should consider guidance on methodologies developed during BEREC's work on QoS in the context of Net Neutrality, especially those found in:

- the 2012 framework for Quality of Service in the scope of Net Neutrality[31];
- the 2014 Monitoring quality of Internet access services in the context of net neutrality BEREC report[32];

30 See Chapter 4.8 *Conclusions and recommendations* of BoR (14) 117 "Monitoring quality of Internet access services in the context of net neutrality"

31 BoR (11) 53, http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/117-a-framework-for-quality-of-srvice-in-the-scope-of-net-neutrality

32 BoR (14) 117, http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/4602-monitoring-quality-of-internet-access-services-in-the-context-of-net-neutrality-berec-report

- the feasibility study of quality monitoring in the context of net neutrality[33]; and
- the BEREC planned 2016-17 workstream on the Regulatory Assessment of QoS in the context of Net Neutrality[34].

163. Following this existing guidance, the speed is calculated by the amount of data divided by the time period. These speed measurements should be done in both download and upload directions. Furthermore, speed should be calculated based on IP packet payload, e.g. using TCP as transport layer protocol. Measurements should be performed beyond the ISP leg. The details of the measurement methodology should be made transparent.

33 BoR (15) 207, http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5576-feasibility-study-of-quality-monitoring-in-the-context-of-net-neutrality

34 BoR (15) 213, section 11.2, http://berec.europa.eu/eng/document_register/subject_matter/berec/annual_work_programmes/5551-berec-work-programme-2016

Article 5
Supervision and enforcement

Article 5(1)

National regulatory authorities shall closely monitor and ensure compliance with Articles 3 and 4, and shall promote the continued availability of non-discriminatory internet access services at levels of quality that reflect advances in technology. For those purposes, national regulatory authorities may impose requirements concerning technical characteristics, minimum quality of service requirements and other appropriate and necessary measures on one or more providers of electronic communications to the public, including providers of internet access services.
National regulatory authorities shall publish reports on an annual basis regarding their monitoring and findings, and provide those reports to the Commission and to BEREC.

Recital 19
National regulatory authorities play an essential role in ensuring that end-users are able to exercise effectively their rights under this Regulation and that the rules on the safeguarding of open internet access are complied with. To that end, national regulatory authorities should have monitoring and reporting obligations, and should ensure that providers of electronic communications to the public, including providers of internet access services, comply with their obligations concerning the safeguarding of open internet access. Those include the obligation to ensure sufficient network capacity for the provision of high quality non-discriminatory internet access services, the general quality of which should not incur a detriment by reason of the provision of services other than internet access services, with a specific level of quality. National regulatory authorities should also have powers to impose requirements concerning technical characteristics, minimum quality of service requirements and other appropriate measures on all or individual providers of electronic communications to the public if this is necessary to ensure compliance with the provisions of this Regulation on the safeguarding of open internet access or to prevent degradation of the general quality of service of internet access services for end-users. In doing so, national regulatory authorities should take utmost account of relevant guidelines from BEREC.

The general approach for supervision

164. With regard to the duties and powers of NRAs set out in Article 5, there are three types of NRA actions to monitor and ensure compliance with Articles 3 and 4.

- Supervision, which encompasses monitoring by the NRA as set out in Article 5(1), and facilitated by the powers to gather information from ISPs in Article 5(2), on:
  - Monitoring of restrictions of end-user rights (Article 3(1)
  - Monitoring of contractual conditions and commercial practices (Article 3(2))
  - Monitoring of traffic management (Article 3(3))
  - Monitoring and assessment of IAS performance and impact of specialised services on the general quality of IAS (Article 3(5) and Article 4)
  - Monitoring of transparency requirements on ISPs (Article 4);
- Enforcement, which can include a variety of interventions and measurements as set out in Article 5(1);
- Reporting by NRAs on the findings from their monitoring, as set out in Article 5(1).

165. To monitor compliance, NRAs may request that ISPs and end-users provide relevant information. Information that can be requested from ISPs is discussed under Article 5(2) and NRAs may collect end-user complaints and ask end-users to complete surveys and questionnaires.

166. Further guidance for specific Articles of the Regulation is described in paragraphs NRAs have the power to collect traffic management information, for instance by:-As well as being published, the reports should be provided to the Commission and to BEREC. To enable the Commission and BEREC to more easily compare the reports, BEREC recommends that NRAs include at least the following sections in their annual reports:, and under Articles 3(2) and 3(5).

Monitoring traffic management practices

167. NRAs have the power to collect traffic management information, for instance by:
    - evaluating traffic management practices applied by ISPs, including exceptions (allowed by Article 3(3) third subparagraph);
    - requesting more comprehensive information from ISPs about implemented traffic management practices, including:
        - a description of, and technical details about, affected networks, applications or services;
        - how they are affected and any other specific differentiation with regards to the application of the practice (such as if the practice is applied only for specific time of day, or in a specific area);
        - in the case of exceptional traffic management practices going beyond those set out in the second subparagraph (Article 3(3)), a detailed justification of why the practice is applied and the time period for which it is applied.
    - requesting records on traffic management measures/practices applied;
    - requesting information from ISPs in following up on complaints received by NRAs;
    - conducting national investigations similar to BEREC's 2012 Traffic Management Investigation[35];
    - collecting information and complaints received directly from end-users or other information sources such as news, blogs, forums and other discussion groups.

35 A view of traffic management and other practices resulting in restrictions to the open Internet in Europe (BoR (12) 30) http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/45-berec-findings-on-traffic-management-pra_0.pdf

168. NRA actions could include conducting technical traffic management measurements, e.g. for detecting infringements such as the blocking or throttling the traffic. NRAs can build on available tools[36], but need to adapt measurements schedules and technical set-ups to specific measurement cases. Measurement results have to be evaluated carefully.

169. NRAs should develop appropriate monitoring policies for detecting infringements of the Regulation and determining necessary actions for guaranteeing that the rights and obligations set out in the Regulation are fulfilled.

Monitoring and assessment of IAS performance

170. IAS performance assessment can be performed at the user or market level:
    - User-level assessment: end-user measurements of the performance of IAS offers can be performed to check whether the ISP is fulfilling his contract. Measurement results are compared to the contracted performance of the IAS offer.
    - Market-level assessment: user-level measurement results are summarised into aggregated values for different categories such as IAS offers, ISPs, access technologies (DSL, cable, fibre etc.), geographical area etc. Aggregated measurement results can be used for market-level assessments.

171. NRAs can use market-level assessment for the regulatory supervision envisaged by Article 5(1) to:
    - cross-check that the published information is consistent with monitoring results (see paragraph NRAs);
    - check that specialised services are not provided at the expense of IAS;
    - check that the performance of IAS is developing sufficiently over time to reflect advances in technology.

172. Market-level assessment data can also be used for:
    - transparency purposes by publishing statistics, as well as interactive maps showing mobile network coverage or average performance in a geographic area for fixed access networks;
    - considering the availability of different IAS offers or offer ranges provided by ISPs, as well as their penetration among end-users;
    - assessing the quality for a specific type of IAS, e.g. based on an access technology (such as DSL, cable or fibre);

36 There are multiple tools available in the market

- comparison of IAS offers in the market;
- investigating possible degradation caused by specialised services.

Monitoring of transparency requirements on ISPs

173. NRAs should monitor transparency requirements on ISPs and could do this by:
    - monitoring that ISPs have specified and published the required information according to Article 4(1);
    - checking that such information is clear, accurate, relevant and comprehensible;
    - cross-checking that the published information is consistent with monitoring results regarding Article 3, such as traffic management practices, IAS performance and specialised services;
    - monitoring that ISPs put in place transparent, simple and efficient procedures to address complaints as required by Article 4(2);
    - collecting information on complaints related to infringements of the Regulation.

Enforcement

174. In order to ensure compliance with the Regulation, and to promote the continued availability of non-discriminatory IAS at levels of quality that reflect advances in technology, NRAs could decide to:
    - require an ISP to take measures to eliminate or remove the factor that is causing the degradation;
    - set requirements for technical characteristics to address infringements of the Regulation, for example, to mandate the removal or revision of certain traffic management practices;
    - impose minimum QoS requirements;
    - impose other appropriate and necessary measures, for example, regarding the ISPs' obligation to ensure sufficient network capacity for the provision of high-quality non-discriminatory IAS (Recital 19);
    - issue cease and desist orders in case of infringements, possibly combined with periodical (daily/weekly) penalties, in accordance with national law;
    - impose cease orders for specific specialised services unless sufficient capacity is made available for IAS within a reasonable and effective timeframe set by the NRA, possibly combined with periodical (daily/weekly) penalties, in accordance with national law;
    - impose fines for infringements, in accordance with national law.

175. In the case of blocking and/or throttling, discrimination etc. of single applications or categories of applications, NRAs could prohibit restrictions of the relevant ports or limitations of application(s) if no valid justification for non-compliance with the Regulation, especially Article 3(3) third subparagraph, is provided. Measures under Article 5(1) could be particularly useful to prohibit practices that clearly infringe the Regulation. Measures could include:
    - prohibiting blocking and/or throttling of specific applications;

- prohibiting a congestion management practice which is specific to individual applications;
- requiring access performance, such as minimum or normally available speeds, to be comparable to advertised/maximum speeds;
- placing qualitative requirements on the performance of application-specific traffic.

176. Requirements and measures could be imposed on one or more ISPs, and it may also, in exceptional cases, be reasonable to impose such requirements in general to all ISPs in the market.

177. The imposition of any of these requirements and measures should be assessed based on its effectiveness, necessity and proportionality:
    - Effectiveness requires that the requirements can be implemented by undertakings and are likely to swiftly prevent or remove degradation of IAS offer available to end-users or other infringements of the Regulation.
    - Necessity requires that, among the effective requirements or measures, the least burdensome is chosen, i.e. other regulatory tools should be considered and deemed insufficient, ineffective or not able to be used fast enough to remedy the situation.
    - Proportionality implies limiting the requirements to the adequate scope, and that the obligation imposed by the requirement is in pursuit of a legitimate aim, appropriate to the pursued aim and there is no less interfering and equally effective alternative way of achieving this aim. For example, if specific ISPs offer degraded IAS services or infringe the traffic management rules of the Regulation, then the proportionate requirements may focus on these ISPs in particular.

Annual reporting of NRAs

178. The reports must be published on an annual basis, and NRAs should publish their annual reports by 30th June for the periods starting from 1st May to 30th April. The first report is to be provided by 30th June 2017, covering the period from 30th April 2016 to 30th April 2017 (the first 12 months following application of the provisions).

179. As well as being published, the reports should be provided to the Commission and to BEREC. To enable the Commission and BEREC to more easily compare the reports, BEREC recommends that NRAs include at least the following sections in their annual reports:
    - overall description of the national situation regarding compliance with the Regulation;
    - description of the monitoring activities carried out by the NRA;
    - the number and types of complaints and infringements related to the Regulation;
    - main results of surveys conducted in relation to supervising and enforcing the Regulation;

- main results and values retrieved from technical measurements and evaluations conducted in relation to supervising and enforcing the Regulation;
- an assessment of the continued availability of non-discriminatory IAS at levels of quality that reflect advances in technology.
- measures adopted/applied by NRAs pursuant to Article 5(1).

Article 5(2)

> At the request of the national regulatory authority, providers of electronic communications to the public, including providers of internet access services, shall make available to that national regulatory authority information relevant to the obligations set out in Articles 3 and 4, in particular information concerning the management of their network capacity and traffic, as well as justifications for any traffic management measures applied. Those providers shall provide the requested information in accordance with the time-limits and the level of detail required by the national regulatory authority.

180. 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) letters (a)-(c). In particular,
        - regarding Article 3(3) letter (a), the exact legislative act, law, or order based on which it is applied;
        - regarding Article 3(3) letter (b), an assessment of the risk for the security and integrity of the network;
        - regarding Article 3(3) letter (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 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.

Article 5(3)

By 30 August 2016, in order to contribute to the consistent application of this Regulation, BEREC shall, after consulting stakeholders and in close cooperation with the Commission, issue guidelines for the implementation of the obligations of national regulatory authorities under this Article.

181. These Guidelines constitute compliance with this provision. BEREC will review and update the Guidelines as and when it considers it to be appropriate.

Article 5(4)

This Article is without prejudice to the tasks assigned by Member States to the national regulatory authorities or to other competent authorities in compliance with Union law.

182. NRAs and other competent authorities may also have other supervision and enforcement tasks assigned to them by Member States in compliance with Union law. Such duties may arise out of, for example, consumer and competition law, in addition to the regulatory framework for electronic communications. Article 5(4) does not affect the tasks of NRAs or other competent national or European authorities arising from such laws, regardless of the fact that such tasks may overlap with the duties of NRAs (or other competent authorities) as set out in the Article. The Regulation does not affect NRAs' or other national authorities' competences to supervise and enforce Directive 95/46/EC or Directive 2002/58/EC referred to in Article 3(4), as such tasks continue to be assigned by national law.

Article 6
Penalties

Member States shall lay down the rules on penalties applicable to infringements of Articles 3, 4 and 5 and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive. Member States shall notify the Commission of those rules and measures by 30 April 2016 and shall notify the Commission without delay of any subsequent amendment affecting them.

183. This provision is aimed at Member States and no guidance to NRAs is required.

Article 10
Entry into force and transitional provisions

Article 10(1)

> This Regulation shall enter into force on the third day following that of its publication in the Official Journal of the European Union.

184. The Regulation entered into force on 29 November 2015.

Article 10(2)

> It shall apply from 30 April 2016, except for the following:
> […]
> (c) Article 5(3) shall apply from 29 November 2015;
> […]

185. The Regulation applies from 30 April 2016, except for Article 5(3) which obliges BEREC to issue these Guidelines and which applies from 29 November 2015.

186. When monitoring and ensuring compliance with Articles 3 and 4, NRAs should take into account that the provisions of the Regulation apply to all existing and new contracts[37] with the exception of Article 4(4), which applies only to contracts concluded or renewed from 29 November 2015. In turn, this means that, for a transitional period, Article 4(4) is not applicable to a certain amount of contracts. However, Article 4(4) will become applicable to more and more contracts over time once they are renewed or newly concluded.

Article 10(3)

> Member States may maintain until 31 December 2016 national measures, including self-regulatory schemes, in place before 29 November 2015 that do not comply with Article 3(2) or (3). Member States concerned shall notify those measures to the Commission by 30 April 2016.

187. Article 10(3) is addressed to Member States. However, when assessing compliance with Article 3(2) and (3), NRAs should take into account that national measures, including self-regulatory schemes, might benefit from a transitional period until 31 December 2016 when they may be maintained, provided that they were in place before 29 November 2015 and have been notified by the respective Member State to the Commission by 30 April 2016. In that event, no

37 See paragraph 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. of these Guidelines

breach of Article 3(2) and Article 3(3) would be found during this transitional period.