Guidelines

on the Implementation of the Open Internet Rules[1]

(Approved by the AKEP Steering Council Decision No. 16 of 8 June 2026)[2]

[1] 1 This document (Main part) has been prepared by AKEP based on the BEREC document "BoR (22) 81 BEREC Guidelines on the Implementation of the Open Internet Regulation", 9 June 2022" making the necessary adjustments to the references of EU Regulation 2015/2120 (Articles 3-5) with the relevant references in Law 54/2024 (Articles 177-179). An integral part of this AKEP Guideline is the appendix at the end of the document: *Appendix 1 AKEP Approach and Plan for the implementation of the Open Internet Guidelines.*

[2] AKEP's position on the comments of interested parties on the Draft Guidelines approved for public consultation with VKD no. 3, dated 2.02.2026, are published in a separate document on the AKEP website https://akep.al/konsultime/konsultime-te-perfunduara/.

Table of Contents

Table of Contents **2**
I. Legal basis, context and general aspects **4**
Terms and Abbreviations 6
II. Subject matter and scope **6**
Definitions 7
III. Safeguarding of open internet access (Article 177) **9**
Article 177(1) End-user rights 10
Article 177(2) Contracts/agreements 12
Article 177(5): beyond reasonable traffic management 23
Article 177(5/a) Union and national legislation 25
Article 177(5/b) Maintaining network integrity 25
Article 177(5/c) Preventing threatening/imminent network congestion 26
Article 177(6) Processing of personal data 27
Article 177(7): Requirement of necessity of specialised services 28
Article 177(8): capacity requirement for specialised services 30
IV. Transparency measures to ensure open internet access (Article 178) **33**
Article 178(1) Transparency measures to ensure open internet access 33
Article 178(1/a) Transparency and traffic management measures 34
Article 178(1/b) Transparency and quality of service parameters 35
Article 178(1/c) Transparency for specialised services 35
Article 178(1/ç) Transparency on contractual speeds 36
Article 178(1/d) Transparency on remedies available to consumers 39
Article 178(2) Procedures to address complaints 39
Article 178(3) The certified monitoring mechanism 40
V. Supervision and enforcement (Article 179) **41**
Article 179(1-2) Supervision and enforcement 41
Article 179(3) Requesting information 46
Article 179(4) Issuing of these Guidelines 47
VI. Entry into force of these Guidelines **48**
APPENDIX 1: AKEP's Approach and Plan for Implementing the Open Internet Guidelines **49**

1. Relation between the AKEP Guidelines on open internet in Albania and the BEREC Guidelines (BoR (22) 81) 49

2. AKEP's approach and plan to implement open internet rules for some specific topics 50

2.1 Specifying minimum speed and NAS in fixed networks 50

2.2 The term “significant, continuous or regularly recurring discrepancy” 52

2.3 IAS (certified) quality measurement mechanism 53

2.4. Publication of AKEP periodic/annual reports regarding the open internet 54

I. Legal basis, context and general aspects

This document "Guidelines on the Implementation of the Open Internet Rules" has been prepared by AKEP pursuant to point 4 of Article 179, of Law No. 54/2024 "On Electronic Communications in the Republic of Albania", and aims to provide clarification of the legal and methodological framework for the implementation of the obligations related to open internet access set out in Articles 177-179 of Law 54/2024.

Articles 177-179 of Law 54/2024 establish the national legal framework for open internet access in Albania, fully aligned with Articles 3-5 of Regulation (EU) 2015/2120,[3] which define the rules for open internet access mandatory to be implemented in all EU Member States. Point 4 of Article 179 of Law 54/2024,[4] which stipulates that AKEP issues guidelines for the implementation of open internet obligations in Albania based on relevant BEREC documents, has been aligned with point 3 of Article 5 of Regulation (EU) 2015/2120,[5] which tasks BEREC with issuing guidelines for the implementation of open internet rules in the EU.

In accordance with point 4 of Article 179 of Law 54/2024, AKEP has prepared this Draft Guidelines document for the implementation of the Open Internet rules in Albania based on the latest BEREC Guidelines on the Implementation of the Open Internet Regulation,[6] making the appropriate adaptations of the references to EU Regulation 2015/2120 (Articles 3-5) contained in the BEREC Guidelines with the relevant references in Law 54/2024 (Articles 177-179).

This document of AKEP aims to provide guidelines for Internet Service Providers (ISPs) and other interested parties on the practical implementation of the obligations provided for in Articles 177-179 of Law No. 54/2024, including:

- ensuring equal and non-discriminatory treatment of traffic when providing Internet access services;
- protecting the rights of end-users;
- ensuring transparency of contractual and technical information, in particular regarding internet service speeds and traffic management practices;
- monitoring compliance and implementing corrective measures.

The AKEP Guidelines aim to ensure:

[3] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and retail charges for regulated intra-EU communications and amending Directive 2002/22/EC and Regulation (EU) No 531/2012.

[4] No later than 6 months after the entry into force of this law, in order to ensure the consistent application of these rules, AKEP, after consulting with interested parties and based on the relevant BEREC documents, shall issue guidelines for the implementation of the obligations under this article.

[5] 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

[6] BoR (22) 81 BEREC Guidelines on the Implementation of the Open Internet Regulation, 9 June 2022

- a unified interpretation of Articles 177–179 of Law 54/2024 with a view to their consistent implementation by all Internet Service Providers (ISPs);
- full harmonisation of the implementation of open internet rules in Albania with BEREC practices and their implementation in EU countries;
- protection of end-user rights;
- transparency and predictability for internet access service providers (ISPs) in the implementation of Articles 177-179 of Law 54/2024.

Document Structure:

This document is structured as follows:

- I. Legal basis, context and general aspects:
  Contains the legal basis and purpose of issuing these guidelines (this part of the document) as well as terms and abbreviations;
- II. Object and scope:
  Clarifications on the object and scope of application of Articles 177-179 of Law 54/2024;
- III. Safeguarding of the open internet access:
  Instructions and clarifications on the definitions of Article 177 (points 1-8) of Law 54/2024;
- IV. Transparency measures for the Open Internet:
  Instructions and clarifications on the definitions of Article 178 (points 1-3) of Law 54/2024;
- V. Supervision and implementation:
  Instructions and clarifications on the definitions of Article 179 (points 1-4) of Law 54/2024;
- VI. Entry into force and transitional provisions:
  Clarifications on the entry into force and implementation of Articles 177-179 of Law 54/2024 and these Instructions;
- APPENDIX 1: AKEP's approach and plan for implementing the Open Internet Rules:
  Contains some additional clarifications to (1) AKEP's Guidelines for implementing the Open Internet Rules in Albania and the connection of these AKEP Guidelines with the BEREC Guidelines, and (2) AKEP's approach and plan for three specific issues related to the open internet in the period 2026-2027 and beyond.

Terms and Abbreviations

2. For the purposes of these Guidelines, the following terms and abbreviations shall have the following meanings:

Application	In these Guidelines, the term "application" is used as short expression for longer expressions used in Articles 177-179 of Law 54/2024, such as "applications and services", "content, application and service".
CAP (Content and Application Provider)	CAPs make content (e.g., web pages, blogs, videos) 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, the term "ISP" is used to refer to providers of Internet Access Service (IAS), on fixed and/or mobile networks. ISPs may also be providers of specialised services.
Specialised services	In these Guidelines, the term "specialised services" is used as an abbreviated expression for "*services other than internet access services, which are optimised for specific content, applications or services or a combination thereof, where optimisation is necessary to meet the requirements of the content, applications or services for a specific level of quality*" (Ref. point 7 of Article 177 of Law 54/2024).
IAS (Internet Access Service)	*"Internet access service" means a publicly available electronic communication service that provides access to the internet, and thereby connectivity to virtually/almost all internet end points, irrespective of the network technology and terminal equipment used;* (Ref. point 62/a of Article 4 of Law 54/2024).

II. Subject matter and scope

3. Articles 177-179, containing the rules for the open internet, which are drafted in accordance with the provisions of Articles 3-5 of Regulation (EU) 2015/2120, AKEP explains that Articles 177-179 of Law 54/2024 aim to establish rules to guarantee *"equal and non-discriminatory treatment of traffic in the provision of internet access services"* and *"the related end-users rights"*. These rules are the same as those applied in all EU countries, according to Articles 3-5 of Regulation (EU) 2015/2120, and are mandatory for implementation by all the undertakings who are internet access service providers.

4. According to the provisions of Law 54/2024 and the BEREC Guidelines, the term 'end-user' includes end-users who are individuals (consumers) and businesses that are end-users of the internet access service (hereinafter, IAS), as well as CAPs..

5. CAPs are protected as end-users under Articles 177-179 of Law 54/2024 to the extent that CAPs use an IAS to reach other end-users. However, some CAPs may also operate their own networks and, as part of this, have interconnection agreements with ISPs; the provision of interconnection service is a wholesale service and distinct from the provision of IAS (which is a retail service).

6. AKEP may consider ISPs' interconnection policies and practices to the extent that they have the effect of restricting the exercise of end-user rights under Article 177(1). For example, this may be relevant in some cases, such as if the interconnection is implemented in a manner that aims to circumvent the provisions of Articles 177-179 of Law 54/2024.

Definitions

Terms used in Articles 177-179 of Law 54/2024

7. The terms used in Articles 177-179 of Law 54/2024 as well as in this Instruction have the same meaning as the terms and definitions given in Article 4 of Law 54/2024, including the terms "end-user", "consumer", "electronic communications services", "electronic communications network" and "network termination point" (Network Termination Point, hereinafter NTP).

Provider of electronic communications to the public

8. The term “provider of electronic communications to the public” (hereinafter PECP) includes both “public communications networks” and “electronic communications services” (ECS), which are defined in Article 4 (points 51 and 62) of Law 54/2024. Therefore, PECP includes both undertakings that are Public Electronic Communications Network Operators and undertakings that are Public Electronic Communications Service Providers (or Network Operators and/or Service Providers).

9. Meanwhile, the definition of PECP does not cover providers of electronic communications services or providers of communications networks that are not publicly available, and therefore, are outside the scope of Articles 177-179 of Law 54/2024.

10. Electronic communications services or networks which are in principle offered by the undertaking to any customer who wishes to be a subscriber/user of the service or network, i.e., not offered only to a predefined group of end-users, are classified as *publicly available (or public)* services/networks. Whereas, electronic communications services or networks which are offered only to a predetermined group of end-users shall be considered not to be publicly available.

11. Virtual private network (VPN) services are typically offered by PECPs to anyone who wishes to enter into a contract for the provision of such a service. In these cases, VPN services will be considered publicly available services; while the operation of a specific VPN constitutes a private network. The term “private” in this context describes the use of such a service which is typically limited (provided only) to the business endpoints that have a contract and have a secure connection for internal communications. VPNs are discussed in more detail in **paragraph 115 of these Guidelines.**

12. The following examples constitute cases that AKEP generally considers as services or networks that are not classified as publicly available (public services/networks):

- internet access service offered by cafes and restaurants to their customers;
- internal networks of corporations/businesses/institutions etc.;
- private M2M networks, for example in factories and ports.

Notwithstanding the above, AKEP may assess in specific cases whether certain services/networks are to be considered public or non-public. In these assessments, AKEP will use criteria such as the contractual relationship under which the service is provided, the range of users and whether this range of users is predetermined or not. Where end-users contract directly with the Internet Service Provider (ISP) specifically for the service being assessed, this service is more likely to be considered a publicly available service. Enterprise services that have a closed group of end-users, which are not available to the general public, will normally not be considered as publicly available services.

"Internet access service"

13. In point 62/a of Article 4 of Law 54/2024, "Internet access service" is defined as *an electronic communication service, available to the public, that provides access to the* ***Internet*** *and thus* ***connection to almost all virtual Internet endpoints***, regardless of the network technology and terminal equipment used.;

14. The term *"internet"* refers to a global system of interconnected networks that enables end users connected to it to communicate with each other. Internet Access Service (IAS) enables such access to the Internet.

15. The phrase "*connectivity* ***to virtually all end-points***" is used because the Internet is a distributed system where a single Internet service provider controls a very limited portion. Due to reasons beyond the control of an individual ISP (e.g., technical limitations, policies of other ISPs, or regulations in some countries), not all endpoints may be reachable/accessible at all times. However, the inability to reach/have access in such cases does not affect the definition or classification of the service as an Internet Access Service (IAS).

16. In cases where the limitations to reach endpoints are due to the use of two different Internet addressing schemes, IPv4 and IPv6, this usually does not mean that the services cannot be defined as IAS. Although two different endpoints with different address types cannot be connected without some translation function, AKEP clarifies that the term "almost all endpoints" does not constitute, under the current rules, a requirement/obligation for ISPs to offer connectivity with both IPv4 and IPv6.

17. Cases where the internet access service enables limited and/or partial access to the internet (sub-internet service), a service which limits access to services or applications (e.g. prohibits the use of VoIP or video streaming) or enables access only to a predefined part of the internet (e.g., access only to certain internet pages), will be considered by AKEP as an internet access service, i.e. which are subject to the rules in Articles 177-178 of Law 54/2024, but the provision of such limited service or offers is contrary to the principle of open internet access and constitutes a violation of Article 177, points 1-5, of Law 54/2024.

These services/offers, referred to as partial/limited Internet access service (sub-internet service), are dealt with in more detail in paragraphs 38 and 55 of this Instruction.

18. Services where the number of accessible endpoints is limited by the nature of the terminal equipment used with such services (e.g., services designed for communication with individual

devices, such as e-book readers, as well as devices for machine-to-machine communication such as smart meters, etc.) are considered outside the scope of Articles 177-179 of Law 54/2024, except when they are used with the intention of circumventing the provisions of Articles 177-179. They may use an IAS (but not provide an IAS nor constitute a substitute for an IAS), may use a private network or constitute a specialised service. If these services use an IAS or constitute a specialised service, the connection service will be subject to the relevant rules applicable to IAS and specialised services in Articles 177-179.

III. Safeguarding of open internet access (Article 177)

19. Article 177 includes measures aimed at guaranteeing open access to the Internet, including the rights of end-users of IAS, as well as obligations and permitted practices for ISPs for open access to the Internet:

- Article 177(1) sets out ***the rights of end-users*** of the IAS;
- Article 177(2) sets out obligations for ISPs on ***the contractual terms*** that may apply to IAS and the commercial practices of ISPs offering IAS, and requires that these **do not restrict the exercise of end-user rights** set out in point 1 of Article 177. When assessing contracts or commercial practices of ISPs, AKEP will take into account the provisions of Article 177 (points 3-5) (see paragraphs 37 and 37a of this Instruction);
- Article 177(3-5) contains obligations on ISPs ***on traffic management practices***, establishing as an obligation that ISPs **must treat all data traffic equally** and providing for specific circumstances in which ISPs may deviate from this rule;
- Article 177(6) sets out the conditions under which traffic management measures may involve the **processing of personal data**;
- Article 177(7-8) defines the freedom or right of ISPs and CAPs to provide ***specialised services***, as well as the conditions under which this freedom may be exercised..

20. Articles 177-179 respect the fundamental rights and principles recognised in the Charter of Fundamental Rights of the EU and the relevant legislation of Albania, in particular the protection of personal data, freedom of expression and information, freedom to conduct a business, non-discrimination and consumer protection..

21. Articles 177-179 of Law 54/2024 do not impose obligations on Internet access service providers (ISPs) to obtain prior (ex ante) authorization or approval from AKEP regarding commercial practices (Article 177(2)), traffic management practices (Article 177(3-5)) or specialised services (Article 177(7-8). However, this does not prevent the exchange of information between AKEP and ISPs on these matters, nor does it prevent AKEP from exercising its obligations or powers to intervene under Article 179 of Law 54/2025.

Article 177(1) End-user rights

1. End users, through the internet access service, have the right ***to access and distribute information and content****,* ***use and provide applications and services****, and* ***use terminal equipment of their choice****, regardless of the location of the end user, the provider or the location, origin, destination of the information, content, application or service..*

22. Article 177(1) defines the rights of end-users in relation to the open internet. The notion of end-user is explained **in paragraph 4** of these Guidelines.

" Access and distribution of information and content"

23. First, end users have the right to access and distribute information and content. "Access and distribution" means that the provisions of Articles 177-179 of Law 54/2024 apply to both the sending and receiving of data via the IAS. "Information and content" is intended to cover any form of data that can be sent or received via the IAS..

" Use and provision of applications and services "

24. Second, end users have the right to use and provide applications and services. "Use and provide" means that the right applies to both the consumption and provision of applications and services. "Applications and services" means both applications (including client and server software) and services.

" Use of terminal equipment at the end user's discretion "

25. Third, end users have the right to use terminal equipment of their choice. Law 54/2024 in Article 3, point 34 has defined the term terminal equipment as follows:

> Article 3 (34). "Terminal equipment" means ***equipment connected directly or indirectly*** to the ***termination point of the public telecommunications network***, which serves for the transmission, reception and (or) processing of information. In any case, the direct or indirect connection may be by wire, optical fiber or electromagnetic means. A connection is indirect if the equipment is located between the termination point and the network interface.

The above definition is a partial approximation of the definition given for "terminal equipment" in point 1 (and point 2) of Article 1 of Directive 2008/63/EC[7] (referred to in Article 2 (41) of the EECC), where the following definitions are given (in bold and underlined the parts that differ/are missing from the definitions in Article 3 of Law 54/2024)

> Article 1 (points 1 and 2) Directive 2008/63/EC
>
> 1."terminal equipment' means:
>
> *(a) equipment directly or indirectly connected to the interface of a public telecommunications network to send, process* ***or*** *receive information; in either case (direct or indirect), the connection may be made by wire, optical fiber or electromagnetically; a*

[7] Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment (OJ L 162, 21.6.2008, p. 20)

connection is indirect if equipment is placed between the terminal and the interface of the network;

(b) ***satellite earth station equipment;***

'satellite earth station equipment' means equipment which is capable of being used for the transmission only ('transmit-only'), or for the transmission and reception ('transmit/receive'), or for the reception only ('receive-only') of radio communication signals by means of satellites or other space-based systems;

AKEP clarifies that for the purposes of implementing Articles 177-179 of Law 54/2024 regarding the definition of 'terminal equipment' it will also take into consideration the above definitions of Directive 2008/63/EC.

As above, the right to choose terminal equipment includes the equipment connected to the public telecommunications network interface or ***network termination point***, which is defined in point 42, Article 3 of Law 54/2024 as follows::

42. "Network termination point" means the physical point at which an end-user has access to the public electronic communications network. In the case of networks involving switching or routing, the network termination point is identified as a specific network address, which may be associated with an end-user number or name.

26. AKEP in assessing whether end-users can use terminal equipment of their choice will assess whether an ISP provides equipment to its subscribers and limits the ability of end-users to replace that equipment with their own equipment, i.e., whether it provides ***"mandatory equipment"***.

27. Furthermore, AKEP will consider whether there is an objective technological necessity for the mandatory equipment to be considered as part of the ISP's network. If there is no necessity, and if the choice of terminal equipment is limited, the practice will be considered by AKEP as a practice in breach of Article 177, point 3. For example, the practice of tethering[8] restriction constitutes a restriction on the choice of terminal equipment because ISPs *"shall not impose restrictions on the use of terminal equipment connected to the network, other than those imposed by manufacturers or distributors of terminal equipment in accordance with European Union law"* (Preamble No. 5 of the EU Regulation).

Legislation relating to the legality of content, applications or services

28. The second subparagraph of Article 3(1) of Regulation (EU) 2015/2120 specifies the following:

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.

This subparagraph clarifies that in EU countries, notwithstanding the provisions of the first subparagraph of Article 3(1) of Regulation (EU) 2015/2120 (Article 177/1 of Law 54/2024) relating to the freedom of end-users/obligation of ISPs to provide open access to the

[8] Tethering allows an end user to use a phone or tablet's internet connection on other devices such as laptops or other phones/devices

internet/without restrictions on content, applications or services), aspects of the legality or illegality of content, applications or services shall be governed by EU law and national law that is compatible with EU law. Regulation (EU) 2015/2120 does not aim to regulate the legality of content, applications or services (ref. Preamble to the EU Regulation).

Although the second subparagraph of Article 3(1) of Regulation (EU) 2015/2120 (the text above) is not included in Article 177, point 1 of Law 54/2024, AKEP clarifies that Articles 177-179 do not aim to regulate the legality or illegality of content, applications or services, which are determined according to the relevant legislation in the Republic of Albania. Therefore, the limitation by ISPs of access to certain content, applications or services that results from the implementation of specific acts for such limitations according to the relevant legislation in the Republic of Albania, does not constitute a violation of point 1 of Article 177 of Law 54/2024 (see also the explanation below).

29. While the second subparagraph of Article 3(1) of Regulation (EU) 2015/2120 contains a clarification regarding the applicability of such legislation, Article 3(3)(a) of Regulation (EU) 2015/2120/EC/EU/EC/Article 177(5)(a) of Law 54/2024 provides for an exemption for ISPs to implement measures that go beyond reasonable traffic management measures in order to comply with the legislation or measures specified in that exemption.

Article 177(2) Contracts/agreements

> *2.* ***Contracts*** *between internet access service providers and end-users* ***on commercial and technical conditions, as well as the characteristics of the internet access service****, such as price, data volume or speed, and any commercial practices used by internet access service providers,* ***do not restrict the exercise of the rights of end-users****, provided for in point 1 of this article.*

30. Article 177(2) clarifies that agreements/contracts between ISPs and end-users on the commercial and technical conditions and characteristics of IAS, such as price, data volumes or speed, and any commercial practices carried out by ISPs are permitted, but must not restrict the exercise of end-users' rights set out in Article 177(1).

31. Article 177(2) contains two important aspects:

- freedom to conclude agreements/contracts between ISPs and end users regarding commercial and technical conditions, as well as the characteristics of IAS;
- determination that such contracts/agreements and commercial practices should not restrict the exercise of end-users' rights set out in Article 177(1).

Agreements/contracts on commercial and technical conditions and characteristics of internet access services

32. Agreements or contracts refer to contractual relationships between ISPs and end-users/subscribers which may include, as defined in Article 177(2), commercial conditions (such as prices), technical conditions (such as data volumes and speed) and any characteristics of the IAS. It should be noted that commercial and technical conditions are often combined in the same contract document.

32a. Where an ISP offers additional end-point-based services (refer to the definition in paragraph 78) together with and in connection with the IAS (regardless of whether the agreement for the provision of additional services is reached at the same time as the IAS subscription contract or at a later stage), such additional services may be assessed by AKEP. ISPs may offer additional services in the same way as CAPs may be offered to third parties. If such additional end-point-based services are part of the contract or are provided in addition to the agreement between the ISP and the end-user, such services must be assessed under Article 177(2).

32b. AKEP, when assessing whether restrictions on such endpoint-based services offered by ISPs as additional services to IAS restrict the exercise of end-users' rights set out in Article 177(1) or create the possibility of circumventing the requirements of Article 177(3-5), may take into account, among others, the following factors:

- if end users continue to have full control of IAS, and can enable and disable endpoint-based blocking by changing settings on the end user's computer, e.g., by configuring the client application software.
- whether the default configuration that the ISP activates for each end-user when offering IAS fully complies with Articles 177(1) and 177(3-5).
- if IAS remains application agnostic and if the commercial and technical conditions of IAS remain constant, independent of any choice of endpoint-based blocking, for example by reducing the price or affecting the QoS of IAS.

If any of these conditions are not met, an ISP will be considered to be in breach of Articles 177-179. Any endpoint-based blocking must also comply with any national provisions on filtering practices, if any. For more details on the assessment of these practices see paragraphs 78-78b.

Commercial practices

33. Commercial practices can consist of all relevant aspects of the commercial conduct of ISPs, including unilateral practices of the ISP[9].

ISP shall not limit the exercise of end-users' of rights.

34. Regarding the characteristics of IAS, the agreement on tariffs for the amount (MB/GB) and specific speed (Mbps/Gbps) of IAS data would not represent a restriction on the exercise of end-user rights. Furthermore, AKEP considers that end-user rights are likely not to be affected, at least in the case where the amount of data, speed characteristics and prices are applied in an application-agnostic manner (see paragraphs 34a and 35). The same assumption applies to the provision of different speeds for different IAS subscription contracts, including in the case of IAS subscription contracts/offers on mobile networks.

34a. In these Guidelines, "application agnostic" means that the commercial and technical treatment of traffic is independent of the application. According to Article 177(2), where the ISP offers more than one level of QoS, application agnostic means that any application can populate any QoS level chosen by the end-user. According to Article 177(3-5), where the ISP offers more than one "traffic

[9] AKEP will also take into consideration the definition of unfair commercial practices under the Albanian consumer protection legislation, which has transposed the EU Unfair Commercial Practices Directive, adapting it in the context of equal and non-discriminatory treatment of IAS traffic by ISPs and the rights of end-users in relation to them.

category", application agnostic means that the treatment of traffic within each category is independent of the applications.

34b. According to Article 177(2), in addition to data volumes and speeds, different levels of QoS parameters, such as latency, jitter, and packet loss, may also be agreed. Such QoS levels should not be confused with the "traffic categories" under Article 177(4) (see paragraphs 57-75). When assessing cases in which ISPs offer different IAS subscription contracts, each with a different QoS level, AKEP will ensure that the implementation of the different QoS levels is application-agnostic and transparent in order to verify compliance with Article 177(3-5). Furthermore, the practice should not restrict the exercise of end-user rights set out in Article 177(1).

34c. If an ISP launches several IAS offers that enable multiple QoS levels at the same time for the same contracted service under Article 177(2), AKEP clarifies that this may be permitted as long as this practice is application-agnostic and complies with the requirements of Articles 177(1) and 177(3-5). In assessing such cases, AKEP may consider, among others, factors such as: end-users should have full control over which applications transmit traffic and with which QoS level (e.g., by configuring the client application software) and that the QoS level at which specific applications are transmitted is not pre-selected by the ISP (e.g., based on a commercial agreement with a third party, such as the end-user on the other side). Such assessment procedures may be detailed by AKEP, if and when ISPs implement new use cases.

34d. In relation to the assessment of the implementation of application-agnostic QoS levels by an ISP, AKEP clarifies that an ISP is not allowed to offer IAS to some end-users with subscription contracts in such a way that would degrade the quality of IAS contracted by other subscribers below the quality levels set out in the terms of the contract agreed pursuant to Article 178(1). AKEP stresses that each ISP must ensure full transparency of the relevant traffic management measures as defined in Article 178(1) of Law 54/2024 (refer to paragraph 135).

According to Article 179(2), AKEP may also impose requirements regarding technical characteristics, minimum quality of service requirements and other appropriate and necessary measures to prevent the degradation of the overall quality of service of internet access services to end-users.

35. Examples of commercial practices that are generally acceptable would include:

- application-agnostic offers where data consumption during a certain period of time (e.g., during weekends or off-peak hours or a certain number of hours per month) is not counted against the overall data limit in effect in the IAS tariff or charged differently, as all traffic is treated equally and no specific application or category of specific applications is treated favourably;
- offers based on different IAS tariffs for different levels of QoS that are independent of applications (for parameters such as speed, latency, jitter, and packet loss, volumes, contract duration, service packages, and packages with or without subsidized equipment, since within a tariff all traffic is treated equally;
- application-agnostic tariff plans for a broad audience (e.g., all consumers) or a target audience group (e.g. special tariffs for young people, schoolchildren, students, the elderly or low-income citizens);
- offers where the internet speed is reduced for the traffic used after the entire amount of data included in the tariff plan has been used; a sufficient speed may still allow internet access

in an application-agnostic manner, this would also allow access to the provider's or application's online self-service portal that allows end users to purchase additional data amounts/packages.

36. An ISP may offer IAS together with an application in a service package. For example, a mobile internet operator may offer a free subscription to a music streaming application for a period of time to all new subscribers. In cases where the traffic related to this application is not subject to any preferential traffic management practice and is not charged/priced differently from the rest of the traffic, such commercial practices are considered not to restrict the exercise of the end-users' rights granted under Article 177(1).

37. In assessing subscription contracts or commercial practices, AKEP will take into account the provisions of Article 177(3-5). In particular, Article 177(3), which obliges ISPs to treat all traffic equally (see paragraph 49). This is in line with the common rules to ensure equal and non-discriminatory treatment of traffic in the provision of internet access services and the rights of end-users related to them, as set out in Article 177(1).

37a. Typically, violations of Article 177(3-5) (e.g. blocking access to certain applications or types of applications or applying differentiated pricing/charging between different applications, i.e., which is not application-independent/agnostic) will be considered to also constitute restrictions on the exercise of end-user rights and constitute a violation of Article 177(2) and 177(1). The rights of end-users set out in Article 177(1) and the obligations of the ISP under Article 177(3-5) cannot be waived even through an agreement/contract or agreed commercial practice between the ISP and the end-user under Article 177(2). This is particularly true because in the provision of internet access services, the principle of equal and non-discriminatory treatment in Article 177 applies to all traffic, and therefore also to traffic transmitted when the ISP is implementing its obligations under an agreement/contract or implementing a commercial practice. More details on the assessment of such cases can be found in paragraphs 49-93 of this Instruction.

38. If an ISP, through contractual terms/conditions (as opposed to technical terms) were to prohibit the use of specific content, or one or more applications/services or categories thereof (for example, by prohibiting the use of VoIP), this would restrict the exercise of the end-user rights set out in Article 177(1). This would be considered as offering a service with limited access to the internet or sub-internet (see paragraph 17).

39. NA (deleted by BEREC).

Guidelines on the assessment of differentiated pricing practices

40. Commercial practices in the provision of services also include differentiated pricing practices. In these offers, the price per data volume (e.g., per GB) is not the same for all data traffic used in a given IAS tariff plan. Differentiated pricing practices can take various forms. For example, the amount of data consumed with an additional data allowance with a given IAS tariff plan does not count towards the overall data cap/maximum amount set in the IAS tariff. This additional data allowance may be unlimited or limited. Furthermore, the price for the additional data allowance above the overall data cap may be zero, positive or negative. Differential pricing practices include both allowed and non-allowable rates.

40a. **Zero-tariff options** are a subset of differentiated pricing practices that are unacceptable. The ECJ has defined zero-rate options as "a commercial practice whereby an internet access provider applies a 'zero rate', or a rate that is more favourable, to all or part of the data traffic associated

with a specific application or category of applications, offered by the partners of that access provider". Therefore, this data is not counted in the volume of data purchased as part of the basic package.

40b. AKEP clarifies that it will consider unacceptable (in violation of Article 177) any differentiated pricing practice for IAS that is not application-agnostic, such as applying a zero price to applications of the ISP itself or of CAPs that subsidize their data.

40c. Unlike (unacceptable) zero-fee options and similar tariff options, there are differentiated pricing practices that are usually acceptable if all elements of the tariff are application-agnostic. Examples of such offers are mentioned above in paragraph 35.

41. An offer with differentiated prices, where all applications are blocked (or slowed down) once the data limit/cap is reached, except for the application(s) for which a zero price or a different price from all other traffic is applied, will be considered by AKEP as a violation of the provisions of Article 177(3) and 177(5) (see paragraph 55).

42. NA (deleted by BEREC)

Guidelines on regulatory assessment by AKEP

43. When assessing ISPs' subscription contracts with end-users or commercial practices in relation to Article 177(2), AKEP's assessment will take into account the purpose of the provisions of Articles 177-179, namely to *"protect the equal and non-discriminatory treatment of traffic"* and to *"guarantee the continued functioning of the internet ecosystem as an engine of innovation"* (Recital 1 of the EU Regulation), as well as Recital 7 of the EU Regulation, which directs intervention against agreements or commercial practices which, *"by reason of their scale, lead to situations where end-user choice is significantly reduced in practice"*, or which would result in *"minimisation of the substance of end-user rights"*.

44. Recital 7 of the EU Regulation also indicates that the assessment should take into account *"the respective market positions of those providers of internet access services and of the providers of content, applications and services involved*".

45. AKEP, when assessing whether an ISP restricts the exercise of end-user rights, will consider the extent to which end-user choice is restricted by the agreed commercial and technical conditions or by the ISP's commercial practices. Not every factor that affects end-users' choices should necessarily be considered as a factor that restricts the exercise of end-users' rights under Article 177(1). The provisions in Articles 177-179 also provide for interference in cases where such restrictions result in a material reduction of choice, but also in other cases that may qualify as a restriction of the exercise of end-users' rights under Article 177(1).

46. As above, AKEP considers that a comprehensive assessment may be necessary for the assessment of such commercial and technical conditions, taking into account in particular:

- the objectives of the EU Regulation/Articles 177-179 of Law 54/2024 and whether the relevant agreements and/or commercial practices bypass or circumvent these general objectives;
- market positions of the ISPs and CAPs involved - a restriction on the exercise of end-user rights is more likely to arise where an ISP or CAP has a 'strong' market position (all other

factors being equal) compared to a situation where the ISP or CAP has a 'weak' market position. Market positions should be analysed in accordance with the principles of competition law;

- the effects on the rights of end-users/subscribers of the consumer and business categories, which include an assessment of, among other things:
    - whether there is any effect on the range and diversity of content and applications that end-users can use and, if so, whether the range and diversity of applications from which end-users can choose is reduced in practice;
    - whether the end user is incentivized to use, for example, certain applications;
    - whether the IAS agreement contains features that significantly reduce end-user choice (see more detail in paragraph 48).
- the effects on the rights of end-users of the CAP, which include an assessment of, among other things:
    - whether there is any impact on the range and diversity of content and applications that CAPs offer, 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 are forced out of the market, or whether there is other material harm to competition in the relevant market;
    - whether the continued functioning of the internet ecosystem as an engine of innovation is affected, for example, whether it is the ISP that chooses the winners and losers, and on the administrative and/or technical barriers that CAPs have to enter into agreements with ISPs.
- the extent of the practice and the presence of alternatives - a practice is more likely to restrict the exercise of end-user rights in a situation where, for example, many end-users are concerned and/or if there are few alternative offers and/or competing ISPs from which end-users can choose.

47. Each of these factors may contribute to a significant reduction in end-user choice and, consequently, to a restriction on the exercise of end-user rights under Article 177(2). In any specific case, the presence of one or more of these factors may in fact restrict the exercise of end-user rights.

48. When conducting such a comprehensive assessment, AKEP may also take into account the following considerations:

- Commercial practices that apply a different price to data associated with a specific application or class of applications are incompatible with the obligation of equal treatment of traffic, as set out in Article 177(3-5).
- In accordance with paragraph 138 (of these Guidelines) on Article 178(1/b) of Law 54/2024, end-users must be informed under which conditions volume-agnostic data usage tariffs apply to applications.

- The assessment of restrictions on end-users exercising their rights may be considered taking into account the actual and potential effects of commercial practices in light of the relevant market and its economic and legal context. To determine whether end-user rights are likely to be harmed in the future, AKEP may consider how the current commercial practice affects the concrete opportunities for potential competitors to enter the relevant market. The assessment of the effect of commercial practices on potential competition would reveal possible restrictions of end-user choice and contribute to "ensuring the continued functioning of the internet ecosystem as an engine of innovation" (Preamble 1 of the EU Regulation). Such an assessment should be supported by evidence or an analysis of the structure of the relevant market (e.g., entry barriers). AKEP can draw on practices from other areas of regulation, such as competition law.

Article 177(3): Equal treatment of traffic

> *3. Internet access service providers, when providing this service,* ***must treat all traffic equally****, without discrimination, restrictions or interference and regardless of the sender and recipient, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used. The designation of this point do not prevent the Internet access service provider from* ***implementing reasonable traffic management measures****, which must be transparent, non-discriminatory and proportionate.*

49. A basic principle of the provisions of Articles 177-179 of Law 54/2024 relates to the obligation of ISPs to treat all traffic equally when providing internet access services. The provisions in Article 177(3) of Law 54/2025 constitute a "general obligation of equal treatment" and that, in principle, "any measure" that is discriminatory by an ISP may be a breach of this general obligation.

AKEP clarifies that the general obligation to treat all traffic equally is not limited to technical aspects or practices of traffic management, but also applies to ISP commercial practices, such as the application of differentiated prices. It therefore also includes unequal treatment through zero-rate options and similar offers (for more details see paragraph 54a below). Usually, breaches of Article 177(3) which are not justified under Article 177(4) and/or Article 177(5) would also constitute a breach of the end-user rights set out in Article 177(1). (see paragraphs 37 and 37a).

50. Since Article 177(3-5) is concerned with the equal treatment of all traffic *"in the course of the provision of an Internet access service" (retail service)*, IP interconnection practices as a wholesale service are not subject to Article 177(3-7).

51. When assessing whether an ISP is acting in accordance with this principle, AKEP will apply a two-step assessment:

- In the first step, it should be assessed whether all traffic is treated equally.
- In a second step, it must be assessed whether the situations are comparable or different and whether there are objective reasons which may justify a different treatment of the different situations (under Article 177(4) – see paragraphs 57-75 below).

52. Furthermore, AKEP will ensure that traffic on an IAS is managed:

- *"without discrimination, restriction or interference";*

- *"regardless of the sender and recipient, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used".*

53. AKEP will consider that equal treatment does not necessarily mean that all end-users will experience the same network performance or quality of service (QoS). Thus, although packets may experience different transmission performance (e.g. in parameters such as latency or jitter), packets can normally be considered to be treated equally as long as all packets are processed without distinction by sender and recipient, by the content accessed or distributed, and by the application or service used or provided.

54. Endpoint-based congestion control[10] (a typical example is Transmission Control Protocol (TCP) congestion control) does not conflict with Article 177(3) since, by definition, it takes place within terminal equipment and terminal equipment is not covered by the provisions of Articles 177-179 (See the explanatory paragraphs regarding Article 177(1) for terminal equipment). AKEP will consider that ISPs' internal network mechanisms that facilitate endpoint-based congestion control are consistent with equal treatment and therefore permissible, as long as these internal network mechanisms are agnostic to the applications running on the endpoints and do not circumvent the provisions of Articles 177-179 of Law 54/2025.

54a. In its decisions of 2 September 2021, the ECJ concluded that a zero-tariff option violates the general obligation to treat all traffic equally under the first subparagraph of Article 3(3) of Regulation (EU) 2015/2120. *The ECJ ruled that "a 'zero-rate' option makes a distinction within the internet traffic, based on commercial considerations, by not counting the basic package traffic for partner applications"* (see also paragraph 40a above). According to the ECJ*, "that the failure, which results from the very nature of such a tariff option because of the incentive it provides, continues regardless of whether or not it is possible to continue to freely access the content offered by the internet access provider's partners after the basic package has been fully used up."*.

55. Agreements/contracts or practices that involve discrimination constitute unequal treatment of traffic and are contrary to Article 177(3-5). This applies in particular to the following examples:

- A practice where an ISP blocks, slows down, restricts, interferes with, degrades or discriminates against access to specific content, of one or more applications (or categories thereof), unless justified under the exceptions in Article 177(5).
- IAS offers where internet access is restricted to a limited set of applications or endpoints by the end-user's ISP (sub-internet service offers) are in breach of Article 177(3), as such offers involve blocking of applications and/or discrimination, restriction or interference with regard to the origin or destination of information.
- An offer with differentiated pricing, where all applications are blocked (or slowed down) once the maximum data limit/limit is reached, except for the application(s) to which a zero price or a different price from all other traffic applies, is considered to be in breach of Article 177(3) and Article 177(5) in a twofold way: There is technical discrimination by blocking (or slowing down) certain types of traffic above the data limit. Furthermore, the price differentiation, which is not application-agnostic, constitutes non-technical unequal treatment of traffic and would lead to the inadmissibility of the offer as a whole (see paragraph 40a above).

56. NA(deleted by BEREC)

[10] *End point-based congestion control*. This should not be confused with *Network-internal congestion management*

Article 177(3-4): Reasonable traffic management

> *3.....*
> *The provisions of this point do not prevent the provider of internet access services from implementing* ***reasonable traffic management measures****, which must be* ***transparent, non-discriminatory and proportionate.***
> *4.* ***Reasonable traffic management measures*** *shall be based on technical quality of service requirements,* ***objectively different for specific categories of traffic*** *and shall not be based on* ***commercial interests****. Such measures* ***shall not monitor specific content*** *and* ***shall not be applied for longer than necessary****.*

Traffic management measures

57. In assessing whether an ISP is acting in accordance with the principle of equal treatment set out in Article 177(3), AKEP shall take into account whether a traffic management measure is a reasonable measure. The principle of equal treatment of traffic does not prevent ISPs from implementing reasonable traffic management measures in accordance with Article 177(4).

"Transparent, non-discriminatory and proportionate" (Article 177(3))

58. When AKEP examines whether a traffic management measure is reasonable, it must first assess whether the traffic management measure is transparent, non-discriminatory and proportionate. These terms are legal principles that are already used in daily regulatory practice when implementing EU legislation and the relevant Albanian national legislation.

59. According to Article 177(3-5), AKEP must require ISPs to provide transparent information regarding traffic management practices and the impact of these practices (see also Articles 178 and 179).

60. When AKEP considers whether a traffic management measure is non-discriminatory, it will take into account the following:

- The obligation for traffic management measures to be non-discriminatory does not prevent ISPs from implementing - with the aim of optimising the overall quality of transmission and user experience - traffic management measures which distinguish between objectively different categories of traffic (see paragraphs 62-67 below).
- Similar situations in terms of similar technical QoS requirements should be treated similarly;
- Different situations in terms of objectively different technical QoS requirements may be treated in different ways if such treatment is objectively justified;
- In particular, the fact that network traffic is encrypted should not be considered by AKEP as an objective justification by ISPs for treating different categories of traffic differently.

61. When AKEP considers whether a traffic management measure is proportionate it will take into account the following:

- The implementation of this measure must have a legitimate purpose by the ISP, i.e. it must contribute to an efficient use of network resources and an optimization of the overall transmission quality;

- The traffic management measure must be appropriate to achieve this purpose (the ISP must have evidence showing that this measure has that effect and that it is not an inappropriate measure);
- Traffic management measures should be necessary to achieve this goal;
- There is no less intrusive and equally effective alternative way of managing traffic to achieve this goal (e.g. equal treatment without traffic categories) with available network resources;
- The traffic management measure must be appropriate, e.g., to balance the competing demands of different traffic categories or the competing interests of different groups.

"Technical QoS requirements, objectively different for specific traffic categories"

62. When assessing whether a traffic management measure is reasonable, AKEP will assess the argumentation presented by the ISP. A traffic management measure, to be considered reasonable, must be based on technical QoS requirements that are objectively different for specific categories of traffic. Examples of technical QoS requirements are latency, speed fluctuation, packet loss and bandwidth.

63. Traffic categories should typically be defined based on QoS requirements, where a traffic category will contain a flow of packets from applications with similar requirements. Therefore, if ISPs implement different technical QoS requirements for specific traffic categories, this should be done objectively by basing them on the sensitivity to the applications' QoS requirements (e.g., latency, jitter, packet loss, and bandwidth). For example, such a category could consist of real-time applications that require a short time delay between sender and receiver.

64. Furthermore, ISPs' traffic management measures are "responsive" to the QoS requirements of traffic categories in order to optimize the overall transmission quality and improve the user experience. To identify traffic categories, the ISP relies on information provided by the application when packets are sent over the network. (See also paragraph 70 regarding information that may legitimately be taken into account by ISPs). Encrypted traffic should not be treated less favourably because of its encryption.

65. When AKEP examines ISPs' internal network mechanisms that assist in endpoint-based congestion control (see paragraph 54) in the context of Article 177(4), the queuing management of different categories of traffic should be assessed according to the same criteria as described generally for Article 177(4).

66. Based on this, reasonable traffic management can be applied to differentiate between objectively different "traffic categories", for example by referring to an application layer protocol or generic types of applications (such as file sharing, VoIP or instant messaging), only insofar as:

- application layer protocol or generic application types require objectively different technical QoS;
- applications with equivalent QoS requirements are treated agnostically in the same traffic category;
- ISP arguments are specific to the objectives pursued by implementing traffic management measures based on different traffic categories.

67. ISPs may prioritize network management and traffic control over the rest of their traffic. Such traffic management practices will be considered reasonable, provided that they are transparent and aimed at properly configuring and securing the network and its equipment by efficiently balancing the load, e.g. by reacting as quickly as possible in case of congestion, failures, outages, etc.

"They are not based on commercial interests"

68. If the traffic management measure is based on the commercial interests of the ISP, the traffic management measure is not considered reasonable. A clear example of this would be where an ISP sets tariffs for the use of different categories of traffic or where the traffic management measure reflects the commercial interests of an ISP that offers certain applications or partners with a provider of certain applications. However, AKEP does not need to prove that a traffic management measure is based on commercial interests; it is sufficient to establish that the traffic management measure is not based on technical QoS requirements that are objectively different.

"They will not monitor specific content."

69. When evaluating traffic management measures, AKEP should ensure that such measures do not monitor specific content (i.e. *transport layer protocol payload*).

70. Conversely, traffic management measures that monitor aspects of traffic other than specific content, i.e. generic content, will be considered permissible. Monitoring techniques used by ISPs that rely on information contained in the IP packet header and the transport layer protocol header (e.g. TCP) may be considered generic content, as opposed to specific content provided by end users themselves (such as text, images and videos).

"Shall not be applied for longer than necessary"

71. AKEP, when assessing traffic management measures, should take into account that such measures should not be applied longer than necessary.

72. The necessary duration of a measure is linked to the principle of proportionality of reasonable traffic management measures in terms of duration, in parallel with the clear precondition "must be proportional" which is linked to their proportionality in terms of scope (type and percentage of traffic affected, impact on the rest of the traffic, equal treatment of comparable situations, etc.).

73. Some traffic management measures are permanently implemented at network nodes as a continuously running queue function, such as packet forwarding rules and associated protocols. However, in packet switched networks, such measures have an effect and affect the technical quality of service of traffic only when necessary, usually in situations of network congestion. For the assessment of the acceptability of traffic management measures, only those situations where the measures have an impact on traffic need to be assessed. Therefore, Article 177(5) does not, in itself, preclude a function that is implemented and in place (but with the traffic management measure not yet effective) on an ongoing basis, insofar as the traffic management measure only becomes effective in times of need. The necessity may materialize several times, or even regularly, over a certain period of time. However, where traffic management measures are in force on a permanent or recurring basis, AKEP should consider whether the traffic management measures can still be qualified as reasonable within the meaning of Article 177(4).

Distinction from exceptional traffic management measures

74. Article 177(5) stipulates, inter alia, that *Internet Service Providers (ISPs) shall not undertake traffic management measures that exceed those set out in point 4 of this Article (177(4))*, and that

traffic management measures such as blocking, slowing down, altering, restricting, interfering with, degrading and discriminating between specific content, applications or services, or specific categories thereof, are prohibited, except in the exceptional cases referred to in points a-c of Article 177(5) explained below..

Distinction from specialised services

75. AKEP clarifies that "traffic categories" should be clearly distinguished from the specialised services mentioned in Points 99 to 115 of these Guidelines. Article 177(7-8) clarifies that specialised services may be provided for optimization reasons in order to meet the requirements for a specific quality level. On the other hand, the use of *"traffic categories"* under Article 177(4) is allowed to contribute to the optimization of the overall quality of the transmission.

Article 177(5): beyond reasonable traffic management

> *5. Internet access service providers shall not take traffic management measures that go beyond those set out in point 4 of this Article, and in particular shall not* ***block, slow down, alter, restrict, interfere with, degrade or discriminate*** *against specific content, applications or services or specific categories thereof, unless and only for as long as necessary, in order for these:*

76. Article 177(5), contains two aspects:

- a prohibition on ISPs from implementing traffic management measures that go beyond reasonable traffic management measures; and
- an exhaustive list of three exceptional cases for which traffic management measures going beyond such reasonable traffic management are permitted.

77. To protect the open internet, Article 177(5) describes traffic management practices that are prohibited, except where there are specific exceptions. These are practices that, among other things, are prohibited, and AKEP will use the following seven fundamental principles in assessing ISPs' traffic management practices:

- no blocking;
- no slowing down;
- no modifying;
- no restricting;
- no interfering with;
- no degrading/impairing; and
- no discrimination

of/between specific content, applications or services, or specific categories thereof.

Blocking, slowing down, altering, restricting, interfering with, impairing/degrading or discriminating constitutes a non-exhaustive list of traffic management measures that are

prohibited, and any other measure that goes beyond reasonable traffic management (under Article 177(4)) is also prohibited.

Practices that do not comply with the seven fundamental principles cited above, or that go beyond reasonable traffic management, may be used by ISPs only based on the three specific exceptions described below under Article 177(5), points (a), (b) and (c).

77a. ISPs may use non-discriminatory data compression techniques on their networks as long as the content originally sent from an endpoint reaches its destination point(s) unmodified, i.e. lossless compression. The use of application-specific downscaling, e.g. to force a CAP to deliver video content at a lower resolution using adaptive bitrate coding, does not constitute data compression.

78. Rules against blocking, slowing down, altering, restricting, interfering with, degrading or discriminating between traffic refer to measures imposed by the ISP on the network when providing an IAS. This means that measures applied to the IP packet in the ISP's network and before the IP packet has reached the destination IP address provided by the end-user's terminal equipment are considered to fall within the scope of Article 177(3-5). These rules apply for example when the processing of application layer protocol elements occurs before the IP packets are received at the destination IP address. Functionality that on the other hand occurs at the destination IP address provided by the end-user computer is called "endpoint-based" in these guidelines and is outside the scope of Articles 177-179 of Law 54/2024.

78a. The default DNS resolvers provided by the ISP when providing IAS are effectively part of the IAS, since these DNS resolvers are installed automatically when the connection is activated and without one, the IAS would be practically unusable for the average end-user. They are therefore considered part of the IAS and the measures implemented by them must comply with Article 177(3-5). Article 177(3-5) also applies to any filtering functionality provided in the modem and access router, in circumstances where these, according to national law and practice, are considered part of the network over which the IAS is provided.

78b. In contrast to measures applied within the network over which the IAS is provided, terminal equipment or client application software-based restrictions imposed by the end-user do not fall within the scope of Articles 177-179 of Law 54/2024 because these measures are executed at the endpoints, i.e. outside the IAS. Such measures may also be applied to the access router when it is considered outside the network according to national law and practice, even though an access router is not an endpoint-based function.

78c. However, as described in point 32a of these Guidelines, ISPs may also offer these endpoint-based services (e.g., to provide parental control or filtering functions together with IAS) in the same way as they are offered by third-party CAPs. Additional DNS resolvers and HTTP proxy servers addressed by the end-user's computer are also examples of such endpoint-based services. On a case-by-case basis, endpoint-based traffic restrictions, such as blocking, should be assessed under Article 177(2) as described in point 32a et seq. of these Guidelines.

79. The three exceptions set out in Article 177(5), paragraphs (a) – (c), have as common prerequisites that the traffic management measure must be necessary to achieve the relevant exception ("**if necessary**") and that it may be applied "*only for as long as necessary*". These requirements stem from the principle of proportionality. Furthermore, as exceptions, they must be interpreted in a strict manner.

80. The prohibition of monitoring specific content does not apply to traffic management that goes beyond reasonable traffic management (that is, traffic management in accordance with the exceptions in (a), (b) or (c)). It should be noted that, according to Article 177(6), any processing of personal data must be carried out in accordance with the law on the protection of personal data (Law no. 124/2024 "On the protection of personal data") as well as the provisions of Law 54/2024 (more specifically Chapter XIX, Protection of personal data and Privacy).

Article 177(5/a) Union and national legislation

> a) shall be in accordance with the relevant legislation and legal and regulatory acts to be implemented by the internet access service provider, including orders of courts or public authorities entrusted with relevant powers;

81. If an ISP implements traffic management measures that cannot be considered as reasonable measures or if an ISP offers a price differentiation that is not agnostic to applications, for example access to a certain application free of charge, AKEP will assess whether an ISP does so because it has to do so for legal reasons, namely to implement relevant legal and/or sub-legal acts, or orders of courts or public authorities entrusted with relevant powers. These exceptional cases also include the implementation by ISPs of the provisions of Articles 149 and 150 of Law 54/2024 regarding the free provision of communications to emergency numbers (the single European number 112 and other national emergency numbers) and communications transmitted for public warnings which rely on internet access.

82. Such measures must comply with the requirements of relevant legal and regulatory acts, including orders of courts or public authorities entrusted with relevant powers.

Article 177(5/b) Maintaining network integrity

> b) to maintain the integrity and security of the network, of the services provided through that network and of the end-users' terminal equipment;

83. Typical attacks and threats that will trigger measures to maintain network integrity and security 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.

84. 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 end points. 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.

85. AKEP should consider that, in order to identify attacks and activate security measures, the use of security monitoring systems by ISPs is often justified. Such traffic management systems consist of two separate components: one component that executes the traffic management itself and one component that monitors traffic on an ongoing basis and triggers the traffic management. Monitoring of traffic to detect security threats may be implemented in the background on a continuous basis. Traffic management measures (such as those listed in paragraph 84) preserving integrity and security are only triggered when concrete security threats 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.

86. Besides monitoring of traffic in order to preserve 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.

87. This exception may be used as a basis for circumventing the provisions of Articles 177-179 of Law 54/2024, as security is a broad concept. Therefore, AKEP will carefully assess whether the requirements of this exception are met and will require ISPs, where necessary, to provide sufficient arguments. In order to assess the security measures, AKEP will take into account the provisions of Law 54/2024, the relevant AKEP Regulation on network security, as well as the relevant acts related to cybersecurity in Albania, including those of AKSK. as well as the "ENISA Guideline for the assessment of security measures in the context of Article 3(3) of the Open Internet Regulation".[11]

Article 177(5/c) Preventing threatening/imminent network congestion

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

88. In exceptional cases, and for no longer than is necessary, ISPs may take traffic management measures beyond those set out in Article 177(4) in order to manage certain types of network congestion, namely threatening network congestion (which can be prevented) and exceptional or temporary network congestion (the effects of which can be mitigated). Threatening network congestion is defined as a situation where congestion is about to materialize quickly, i.e. it is inevitable.

89. Actions to prevent threatening (imminent) network overloads are implemented only in cases of extraordinary and temporary overloads.

90. AKEP, when assessing the exceptions to congestion management under Article 177(5)/c, shall refer to the general criteria of strict interpretation and proportionality set out in Article 177(5). Furthermore, AKEP shall check that congestion management is not used to circumvent the prohibition of congestion, restriction and discrimination of traffic.

[11] ENISA "Guideline on assessing security measures in the context of Article 3(3) of the Open Internet regulation"

91. Due to the requirement that exceptional traffic management may be applied only as and when necessary and only for as long as necessary, NRAs should consider that in cases where non-application-specific congestion management (that is, congestion management that does not target specific applications or categories of applications) is not sufficient, the congestion may be dealt with under Article 177(5)(c). Furthermore, in such cases, equivalent categories of traffic should be treated equally. If possible, any mitigation action should be limited to the part of the network where the congestion occurs

92. Congestion management can be done on a general basis, independently of applications. AKEP will examine whether such types of congestion management would be sufficient and equally effective to manage congestion, in light of the principle of proportionality. For the same reason, AKEP will examine whether traffic limitation, as opposed to traffic blocking, would be sufficient and equally effective to manage congestion.

93. As part of the review of congestion management practices, AKEP may monitor that ISPs are appropriately sizing their network and taking 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;
- application-specific congestion management should not be applied or accepted as a substitute for more structural solutions, such as expansion of network capacity.

Article 177(6) Processing of personal data

> *6. Any traffic management measure that may require the processing of personal data may be taken only if such processing* ***is necessary and proportionate*** *to achieve the objectives set out in point 3 of this Article. Such processing shall be carried out* ***in accordance with the law on the protection of personal data****, this law, and the acts implementing them.*

94. Personal data may be processed during traffic management. Article 177(6) provides that such measures may process personal data only if certain requirements are met and only under certain conditions.

95. Article 177(3-5) distinguishes between reasonable traffic management measures and traffic management measures that go beyond reasonable traffic management measures. Article 177(6) applies to both of these forms of traffic management ("*any traffic management measure*"). With regard to reasonable traffic management measures, these requirements are further specified by Article 177(4) which states that *"such measures shall not monitor specific content"*.

96. The objectives referred to in Article 177(6) are the same as those set out in Article 177(3-5).

"Necessary and proportionate"

97. The processing of personal data within the course of traffic management is also subject to the proportionality requirement. AKEP should assess whether the processing of personal data undertaken by ISPs is necessary and proportionate to achieve the objectives set out in Article 177(3-5).

"Compliance with data protection law"

98. The processing of personal data within the framework of traffic management by ISPs must be in accordance with Law No. 124/2024 "On the Protection of Personal Data") as well as the provisions of Law 54/2024 (more specifically Chapter XIX, Protection of Personal Data and Privacy). For the implementation of Law No. 124/2024 and the relevant sub-legal acts within the framework of Article 177 of Law 54/2024, AKEP will cooperate with the Commissioner for the Right to Information and Personal Data Protection, as the competent authority for supervising the implementation of Law 124/2024.

Article 177(7): Requirement of necessity of specialised services

7. 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 optimized for specific content, applications or services, or a combination thereof, where the optimization is necessary in order to meet requirements of the content, applications or services for a specific level of quality.

99. Beyond the delivery of applications through the IAS, there can be demand for services that need to be carried at a specific level of quality that cannot be assured by the standard best effort delivery.

100. 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).

101. These providers are free to provide the services referred to in Article 177(7-8), which in this Directive are called specialised services, only when certain requirements are met. Article 177(7-8) provides protection for the provision of specialised services which are characterised by the following characteristics referred to in Article 177(7):

- 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.

102. Their provision is subject to a number of conditions in Article 177(8), 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.

103. Specialised services should not be used to circumvent the provisions regarding traffic management measures applicable to IASs.

104. All of these safeguards aim to ensure the continued availability and overall quality of IAS based on best efforts.

105. AKEP in such cases will verify whether the application can be provided via IAS at the specific quality levels that are objectively necessary in relation to the application, or whether they are designed to circumvent the provisions regarding traffic management measures applicable to IAS, where the latter is not permitted, as it is contrary to Articles 177-179 of Law 54/2024..

Assessment according to Article 177(7)

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

107. AKEP, when assessing whether the practices used to provide specialised services comply with Article 177(7), shall apply the method set out in paragraphs 108-115 of this Instruction.

108. AKEP may request from the provider relevant information regarding their specialised services, using the powers granted by Article 179(3). In their responses, providers must provide information regarding their specialised services, including what are the relevant quality levels, not provided by the IAS (e.g. delay, jitter and packet loss), but also other resource management requirements as explained in paragraph 108a below, and any contractual requirements. Furthermore, the "specific quality level" must be specified, and it must be demonstrable that this specific quality level cannot be ensured through IAS and that the quality requirements are objectively necessary to ensure one or more key characteristics of the service.

108a. Requirements for a specific quality level may not only refer to standard parameters such as speed, latency and jitter, but may, for example, also apply to other quality parameters in new networking paradigms, such as machine-to-machine (M2M) services. In such cases, devices may have limited resources (e.g., limited processing power, battery life and memory capacity) and the provision of services over the network may have to deal with issues such as power depletion, interference and security to maintain a specific quality level. Addressing these issues is essential to ensure the specified level of service quality, and specialised services may be justified in cases where requirements cannot be met by IAS for resource-limited devices.

109. Based on this information, AKEP will assess the requests referred to in Article 177(7).

110. If the provision of a specific level of quality is objectively necessary, this cannot be provided simply by giving it general priority over comparable content. Specialised services do not provide general connectivity to the Internet (see also paragraph 115 on VPN services for further clarification) and they may be provided, for example, over a connection that is logically separate from IAS traffic in order to ensure these levels of quality.

110a. Regarding the internet connectivity, a dedicated connection between servers at the application layer (for example, allowing VoLTE subscribers to call OTT VoIP users) would not provide general connectivity between internet endpoints, i.e. the service would not be usable or offered as a replacement for IAS. Therefore, a specialised service could rely on such a connection.

110b. Regarding the example of logical separation of traffic between specialised services and IAS, usually when the two categories of services are provided over a common infrastructure, it should be noted that the logical separation can be provided with fixed or dynamic capacity or without reservation of capacity for IAS versus specialised services. However, the ISP is obliged to provide the quality of IAS as specified under the transparency requirements in Article 178. Furthermore,

the rules in Article 177(8) stipulate that specialised services shall not be provided to the detriment of the overall quality of IAS for end-users.

111. AKEP will verify whether, and to what extent, the optimised provision is objectively necessary to ensure that the requirements of one or more specific and essential characteristics of content, applications and services are met, and to enable end-users to be given an appropriate assurance of quality. To do so, AKEP will assess whether an electronic communications service, other than IAS, requires a level of quality that cannot be provided through an IAS. If not, these electronic communications services are likely to circumvent the provisions of Articles 177-179 of Law 54/2024 and will therefore not be permitted. In the assessment, AKEP will take into account that different network technologies may offer different levels of performance.

112. The Internet and the nature of IAS will evolve over time. A service that is considered to be a specialised service today may not necessarily qualify as a specialised service in the future due to the fact that optimization of the service may not be objectively necessary, as the overall standard of IAS may have improved. On the other hand, other services may emerge that need to be optimized, even as the standard of IAS improves. AKEP will assess whether a service qualifies as a specialised service on a case-by-case basis. In the event of a reassessment, this is expected to take place over a longer period of time. AKEP clarifies that it will not keep specialised services under constant review. Where AKEP assesses that a service no longer qualifies as a specialised service due to the improved quality of the IAS, the ISP will be allowed a reasonable transitional period for the gradual phasing out of the specialised service. In such cases, the relevant administrative procedures will apply, including respect for the principle of proportionality.

113. **Typical examples of specialised services** offered to end users are VoLTE services and linear IPTV streaming with specific QoS requirements, provided that they meet the requirements of Articles 177-179 of Law 54/2024, in particular Article 177(7). Under the same preconditions, other examples would include real-time health services (e.g. remote surgery) or *"certain services responding to a public interest or certain new machine-to-machine communication services"***.**

114. QoS can be particularly important for corporate customers, and these customers may need specialised services which - since they are aimed at businesses - are often called "business services". Such "business services" cover a wide range of services and should be evaluated on a case-by-case basis.

115. VPNs may qualify as specialised services in accordance with Article 177(7) of Law 54/2024. However, to the extent that corporate services, such as VPNs, also provide access to the internet, the provision of such internet access by a provider of electronic communications to the public must be analysed under Article 177(1) to (6) of Law 54/2024. For example, such specialised services cannot be used to replace an IAS with a service that prioritises specific applications while providing access to the interne.

Article 177(8): capacity requirement for specialised services

> *8. 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.*

Sufficient network capacity for specialised services in addition to IAS

116. 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.

117. In a network with limited capacity, IAS and specialised services may compete for the general network resources. In order to protect the availability of the general quality of IAS, Article 177(8) does not allow the provision of specialised services if the network capacity is not sufficient to provide them in addition to any IAS provided, because this would lead to the deterioration of the IAS and thus circumvent the provisions of Articles 177-179 of Law 54/2024. Articles 177-179 of Law 54/2024 protect the general quality of IAS, and not specialised services, from deterioration.

118. AKEP will assess whether, in order to ensure the quality of specialised services, Internet service providers have provided sufficient network capacity for each IAS offer provided through the infrastructure, as well as for specialised services. If not, the provision of specialised services is not permitted according to the provisions of Articles 177-179 of Law 54/2024.

119. AKEP may request information from ISPs regarding how sufficient capacity is provided and to what extent the service is provided (e.g., networks, coverage and end users). AKEP may 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.

120. AKEP will assess whether there is sufficient capacity for IAS when providing specialised services, for example by carrying out IAS measurements (see paragraphs 174-176). In these measurements, AKEP will take into account/use the relevant methodologies developed by BEREC for Net Neutrality QoS in recent years.

"Not to the detriment of the availability or general quality of IAS for end-users"

121. 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(s) (i.e. its availability and general quality) and whether there is sufficient capacity to provide specialised services in addition to IAS. NRAs may consider that IAS quality measurements could be performed with and without specialised services, both in the short term and in the long term, which may include measurements before the specialised services are introduced in the market as well as after.

121a. BEREC is in the process of developing a tool for measuring net neutrality and will seek to use this work to further develop the measurement methodology in relation to measuring the overall quality of IAS. AKEP will participate in this collaboration and take into account the results of this work when available. AKEP may also collect information from ISPs to assess and measure the impact of specialised services on the overall quality of IAS.

122. The end-user may determine for himself how to use the dedicated part of an end-user's capacity while IAS and specialised services compete directly for it. Where it is technically

impossible to provide the specialised service in parallel with IAS without impairing the quality of the end-user's IAS, AKEP shall not consider such competition for capacity as a breach of Article 177(8), as long as the end-user is informed in accordance with Article 178(1)(c) of the impact on his IAS and can obtain the internet speeds under the contract for any IAS subscribed in parallel. Where the activation of a specialised service by an individual end-user affects only his IAS, AKEP shall not consider it to be detrimental to the overall quality of the IAS. However, the detrimental effects shall not occur in those parts of the network where capacity is shared between different end-users.

123. Also, in mobile networks - where the number of active users in a given cell, and consequently the traffic volumes, are more difficult to predict than in fixed networks - the overall quality of IAS for end-users should not be considered to cause harm when the overall negative impact of specialised services is unavoidable, minimal and limited to a short duration. In contrast, such unpredictable circumstances related to the number of users and traffic volumes should not normally occur in fixed networks.

124. AKEP may assess whether the provision of specialised services reduces the overall quality of the IAS, for example, by assessing the extent to which measured download or upload speeds decrease or delays, latency variations, or packet loss increase. Normal small-scale temporal fluctuations or normal small-scale changes across the network should not be considered detrimental to overall quality. Network outages and other temporary problems caused by network faults, for example, should be treated separately.

125. AKEP will intervene if persistent and significant performance degradations are detected for IAS. This can be detected if the measured performance is consistently above an average level (for parameters such as latency, jitter or packet loss) or below an average level (for parameters such as speed) previously detected over a relatively long period of time, such as hours or days), or if the difference between the measurement results before and after the start of the provision/use of the specialised service is statistically significant. In the case of short-term assessments, the difference between the measurement results with and without the specialised service should be assessed in a similar manner.

“Not be usable or offered as a replacement for IAS”

126. It is very important that the provisions regarding specialised services do not serve as a potential circumvention of Articles 177-179 of Law 54/2024. Therefore, AKEP will assess whether a specialised service is a potential substitute for IAS, and whether the capacity needed to provide it is at the expense of the capacity available for IAS.

127. An important aspect that AKEP will assess to decide whether a specialised service is considered a substitute for an IAS is whether the service actually offers internet access, but in a limited manner, with a higher quality or with differentiated traffic management. If so, this would be considered a circumvention of Articles 177-179 of Law 54/2024.

IV. Transparency measures to ensure open internet access (Article 178)

Article 178(1) Transparency measures to ensure open internet access

> 1. Providers of internet access services shall ensure that any contract which includes internet access services specifies at least the following:
> (the information requirements in paragraphs (a)-(d) of Article 178(1))

128. AKEP shall ensure that ISPs offering IAS to all end-users (e.g. consumer end-users and business customers) include in contracts for IAS the relevant information referred to in Article 178(1)(a-d) in a clear, comprehensible and comprehensive manner, and publish this information on their website.

129. AKEP clarifies that the transparency requirements for ISPs in relation to IAS set out in Articles 178(1) and 178(2) are additional requirements to those provided for in Chapter XVI or XVIII of Law 54/2024. AKEP may also establish additional monitoring, information and transparency requirements, including those relating to the content, form and manner of information to be published.

130. In order for the information referred to in Article 178 to be clear and understandable:

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

131. AKEP clarifies that ISPs have an obligation to include in the contract and publish the information referred to in Article 178(1) (a) to (d). This can be presented in two parts (levels of detail):

- The first part may provide high-level (general) information. The information about the IAS provided should include, for example, an explanation of the speeds, examples of known applications that can be used with sufficient quality and an explanation of how such applications are affected by the limitations of the IAS provided. This part should include a reference to the second part where the information required by Article 178(1) of the Regulation is provided in more detail.
- The second part may consist of more detailed technical parameters and their values, as well as other relevant information required by Article 178(1) of Law 54/2024 and in these Guidelines.

132. If necessary, AKEP will provide examples of how information can be provided in a transparent manner, taking into account best practices in EU countries and BEREC guidelines on net neutrality transparency..

133. Terms of subscription contracts that would exclude or inappropriately restrict the exercise of the end-user's legal rights vis-à-vis the ISP in the event of the ISP's total or partial or inappropriate non-fulfilment of any of the contractual obligations shall be considered unfair under Articles 177-179 of Law 54/2024, including the application of the relevant legislation on consumer protection and unfair terms in consumer contracts.

134. The provisions of Article 178(points 1 and 2) of Law 54/2024 shall apply to all contracts regardless of the date of conclusion or renewal of the contract. The provisions of Article 178, point 3, shall apply only to contracts concluded or renewed from 20.12.2025, in accordance with the deadline provided for in the law and with the explanations provided in these Guidelines, in particular in paragraphs 160–166 and in Appendix no. 1

Article 178(1/a) Transparency and traffic management measures

> 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;

135. ISPs are obliged to include in the contract and publish a clear and comprehensive explanation of the traffic management measures implemented in accordance with Article 177(4-5), including the following information:

- how traffic management measures may affect the end-user experience in general and in relation to specific applications (e.g. where specific categories of traffic are treated differently in accordance with Article 177). Practical examples should be used for this purpose. In particular, the following information should be provided by the ISP:
    - the download and upload limits that apply to the IAS selected by the end-user, the traffic management used to manage compliance with download limits, and the circumstances under which these apply.
- the circumstances and manner in which traffic management measures are implemented which may have an impact as provided for in Article 178(1)(a);
- how traffic management measures can affect the QoS of IAS, especially in cases of network congestion and also in relation to other internet access services with different QoS parameters, where the ISP offers multiple internet access services with different QoS parameters;
- any measures implemented when managing traffic that uses personal data, the types of personal data used, and how ISPs ensure the privacy of end users and protect their personal data when managing traffic.

136. The information shall be clear and comprehensive. The information shall not consist merely of a general condition setting out the possible impacts of traffic management measures that may be implemented in accordance with Articles 177 to 179. The information shall also include, at

least, a description of the possible impacts of traffic management practices that are in force in the IAS.

Article 178(1/b) Transparency and quality of service parameters

> 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;

137. Besides speed, the most important QoS parameters for internet access are delay, delay variation (jitter) and packet loss. These other QoS parameters should be described if, in practice, they could have an impact on IAS and application usage. ISPs should provide end-users with information that is based on the effects. End-users should be able to understand the implications of these parameters on application usage and whether certain applications (e.g., interactive voice/video communication or 4K video streaming) cannot actually be used due to high latency or slow IAS speeds. ISPs may provide categories of applications or known examples of such applications that could be affected by the above.

138. Regarding volume limits, contracts should specify the "size" of the upper limit (in quantitative terms, e.g. GB), what this means in practice and the consequences of exceeding it (e.g., additional charges, speed restrictions, blocking of all traffic, etc.), as well as, in the case of price differentiation, a clear explanation of which data is counted against which limit or for which price. For example, if the user receives unlimited internet access for a limited period of time, there should be a clear explanation of the different time periods and what pricing applies to data during different time periods. When specifying speeds in a contract and publishing information, it should be taken into account whether the speed will be reduced after a certain data limit has been reached. ISPs can also provide information and examples about the type of data usage that would lead to a situation where the data limit is reached (e.g. how many GB can be consumed on average during 1 hour using popular applications, such as SD, HD, 4K video streaming or how long it takes on average to reach the data limit using these applications).

AKEP clarifies that the definitions of this point include both data limits/restrictions on mobile networks and those on fixed networks, published as unlimited, but for which fair usage policies apply.

Article 178(1/c) Transparency for specialised services

> c) a clear and understandable explanation of how any service referred to in point 7 of Article 177 of this Law, to which the end-user agrees, may in practice have an impact on the internet access services provided to that user;

139. ISPs must include in the contract and publish clear and understandable information on how the specialised services included in the end-user subscription contract may affect the IAS. This is discussed further in paragraph 122.

Article 178(1/ç) Transparency on contractual speeds

> ç) a clear and understandable explanation of the **minimum, normally available, maximum and declared** download and upload speeds of internet access services **in the case of fixed networks**, or of the **estimated and declared maximum download and upload speeds** of internet access services **in the case of mobile networks** and how significant deviations from the respective declared download and upload speeds affect the exercise of end-user rights, set out in point 1 of Article 177 of this Law;

140. In order to empower end-users, the speed values required by Article 178(1)(ç) must be specified in the contract and published in such a way that they can be verified and used to determine any discrepancies between the actual performance and that agreed in the contract. Upload and download speeds must be provided as single numerical values in bits/second (e.g. Mbps or Gbps for speeds >=1Gbit/s). Speeds must be specified based on the transport layer protocol payload and not based on a lower layer protocol.

141. In recent years, products have been introduced to the market that include a combination of different types of technologies and, in some cases, a mix of fixed and mobile technologies. Despite innovative forms of Internet connectivity, the end user needs to be informed about what level of service they can expect. ISPs, when introducing a new product to the market, can implement their offering using their chosen technologies, as long as they are transparent about the actual performance of the IAS. In order for contractual speed values to be understandable, contracts should specify factors that may have an impact on speed, both within and outside the ISP's control. This also applies to FWA (Fixed Wireless Access) and services that use a combination of technologies such as hybrid IAS, where unpredictable influences (for example environmental conditions) may affect service delivery to a certain extent.

141a. AKEP will consider certain types of FWAs as fixed network services for the purpose of the transparency requirements in Article 178. This is the case, for example, where a network using wireless technology (including mobile network) is used for the provision of IAS at a fixed location with dedicated equipment and either capacity reservation or the use of a specified frequency spectrum band is applied. In this case, the provision of relevant information should be in line with the transparency requirements for fixed networks. When AKEP will examine a specific case, it will take into account the manner of implementation and the specific conditions of the product.

141b. AKEP will consider hybrid access as fixed network access for the purpose of the transparency requirements in Article 178 when it consists of a combination of fixed and mobile technologies as a single subscription, is offered at a fixed location and is marketed as a fixed service. Therefore, the information provided in such cases should be in line with the transparency requirements for fixed networks. If this is not the case, the fixed part of the service should meet the transparency requirements of the fixed network and the mobile part of the service should meet the transparency requirements of the mobile network. For example, in relation to the mobile component of a hybrid IAS when marketed separately from the fixed component, AKEP may impose obligations in relation to minimum quality of service requirements and other appropriate and necessary measures under Article 179(1)..

142. AKEP clarifies that the obligation on ISPs to include in the contract and publish information about the declared/advertised speeds does not imply a requirement to advertise the speeds; rather, it is limited to including in the contract and publishing information about the speeds that 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 is advertised. An ISP may of course also advertise other IAS offers with higher or lower speeds that are not included in the contract to which the subscriber is a party (either by choice or due to the unavailability of the service in his location), in accordance with the norms governing marketing.

Specifying speeds for an IAS in the case of fixed networks

Minimum speed

143. The minimum speed is the lowest speed that the ISP undertakes to provide to the end user, according to the contract that includes the IAS. In principle, the actual speed should not be lower than the minimum speed, except in cases of IAS interruption. If the actual speed of an IAS is significantly, and continuously or regularly, lower than the minimum speed, this would indicate a performance discrepancy with respect to the agreed minimum speed.

144. AKEP may impose requirements for the determination of the minimum speed under Article 179(2), for example that the minimum speed be in reasonable proportion to the maximum speed. For this please refer to Appendix 1 of this document.

Maximum speed

145. The maximum speed is the speed that an end-user could expect to receive 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.

146. AKEP may impose requirements for the determination of the minimum speed under Article 179(2), for example that the minimum speed be in reasonable proportion to the maximum speed. For this please refer to Appendix 1 of this document.

Normally available speed

147. The normally available speed is the speed that an end user can expect to receive most of the time when using the IAS service. AKEP explains that the normally available speed has two dimensions:

- numerical value of speed, and
- the availability (as a percentage) of speed during a given period, such as peak hours or throughout the day.

148. The normally available speed must be available during the specified daily period. AKEP may impose requirements for the determination of normally available speeds under Article 179(2). For this please refer to Appendix 1 of this document.

Examples include:

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

149. To be meaningful, the end user must be able to assess the value of the normally available speed compared to the actual performance of the IAS based on the information provided.

Declared (advertised) speed

150. The declared (advertised) speed is the speed that an ISP uses in its commercial communications, including advertising and marketing, in relation to the promotion of IAS offers. Where speeds are included in the marketing of an offer by an ISP (see also paragraph 142), the advertised speed must be specified in the published information and in the contract for each IAS offer.

151. AKEP may impose requirements in accordance with Article 179(2) on how the speeds specified in the contract relate to the advertised speeds, for example that the advertised speed must not exceed the maximum speed specified in the contract, i.e., the maximum speed must be equal to the declared/advertised speed.

Specifying the speeds of an IAS in mobile networks

152. The maximum download and upload speeds envisaged and advertised must be described in contracts according to paragraphs 153-157.

Estimated maximum speed

153. The maximum rated speed for a mobile IAS should be specified so that the end-user can understand the maximum speed realistically achievable for his contractual relationship with the operator in different locations and under realistic usage conditions. The maximum rated speed may be specified separately for different network technologies (3G, 4G or 5G) which affect the maximum speed available to an end-user. End-users should understand that they may not be able to achieve the maximum speed if their mobile terminal does not support that speed.

154. AKEP may impose requirements for the determination of maximum rated speeds under Article 179(2).

155. Estimated maximum download and upload speeds on the mobile network may be made available/published by mobile operators on a geographical basis, providing mobile IAS coverage maps with estimated/measured network coverage speed values in all locations.

Declared/advertised speed

156. The advertised speed for a mobile IAS offer should reflect the speed that the ISP is actually able to deliver to end-users. Although 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 that they are able to assess the value of the advertised speed compared to the actual performance of the IAS. Mobile operators should specify important factors that limit the speeds achieved by end-users.

157. AKEP may impose requirements in accordance with Article 179(1-2) on how speeds specified in the contract relate to advertised speeds, for example that the advertised speed for an IAS, as specified in a contract, must not exceed the maximum speed provided for as specified in the same contract. See also paragraph 142 and Appendix 1.

Article 178(1/d) Transparency on remedies available to consumers

> d) a clear and comprehensible explanation of the remedies available to the consumer, in accordance with national law, in the event of any persistent or regularly recurring discrepancy between the actual performance of the internet access service, in terms of speed or other quality of service parameters, and the required performance, in accordance with the above subparagraphs.

158. National legislation on legal remedies available to the consumer in the event of any persistent discrepancy between the actual and contracted performance of the internet service includes the provisions of Law 54/2024 (Article 46) as well as the relevant sub-legal acts of AKEP for consumer/subscriber protection containing provisions regarding the handling of complaints and the resolution of disputes between end users and undertakings, as well as in the general legislation on consumer protection. Also, in addition to Articles 177-179, Law 54/2024 contains specific obligations for ISPs for internet access services, including on the information that ISPs shall include in the subscription contract with the end-user under Article 180, point 1/ç (*any compensation and reimbursement agreement, including where applicable, a clear reference to the rights of consumers, which apply if the contracted service quality levels are not met)*, point 2/a/i (*any minimum level of service quality to the extent that these are offered and taking into account the BEREC guidelines regarding internet access services: low latency, jitter, packet loss*).

Examples of possible remedies for a discrepancy between contracted and actual speeds that ISPs may offer to end-users/subscribers are price reduction, early termination of the contract without penalty to the subscriber, compensation to the subscriber or correction of the performance discrepancy, or a combination thereof.

AKEP will ensure that ISPs provide consumers with information specifying such legal remedies, within the framework of drafting the sub-legal acts for the implementation of Law 54/2024.

Article 178(2) Procedures to address complaints

> 2. Internet access service providers shall provide transparent, simple and efficient procedures for handling user complaints regarding the rights and obligations set out in Article 177 of this Law and point 1 of this Article, which shall be published on their website and made available at points of sale.

159. ISPs are required to adhere to certain good practices regarding complaint handling procedures, such as:

- informing end-users in the contract, as well as on their website, in a clear manner, about the procedures 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 post or telephone;
- providing a single point of contact for all complaints relating to the provisions set out in Article 177 and Article 178(1), regardless of the nature of the complaint;

- enabling the end user to be able to inquire about the status of their complaint in the same manner in which the complaint was raised;
- informing end users about the response to the complaint in a relatively short time, considering the complexity of the issue;
- informing the end user about the means to resolve disputes under Law 54/2024 (Article 46) and the relevant sub-legal acts (AKEP Regulation on the protection of consumers/subscribers) or consumer protection legislation, i.e. if the end user believes that the complaint has not been properly handled by the ISP/is not satisfied with the solution provided by the ISP, he/she has the right to request the resolution of the dispute from AKEP.

Additional transparency requirements

160. ISPs' obligations regarding transparency and publication of information to end-users regarding internet access services, including complaints and resolution of disputes between end-users and undertakings, are part of Law 54/2024 and the relevant sub-legal framework.

Article 178(3) The certified monitoring mechanism

> 3. Any significant, persistent or regularly recurring discrepancy between the actual quality of the internet access service, in relation to speed or other quality of service parameters and the performance demonstrated by the internet access service provider, in accordance with points (a) to (d) of point 1 of this Article, where the relevant facts are verified by a monitoring mechanism certified by AKEP, shall be deemed to constitute a performance discrepancy for the purposes of invoking the legal remedies available to the consumer, in accordance with national legislation. This paragraph shall apply only to contracts concluded or renewed 1 year after the entry into force of this Law.

161. The relevant facts establishing a significant non-compliance may be determined by any monitoring mechanism certified by AKEP, whether operated by AKEP or by a third party. Point 3 of Article 178 of Law 54/2024 (cited above) does not impose an obligation on AKEP to make available itself or to certify a third party monitoring mechanism, or how the certification should be carried out. If AKEP provides a monitoring mechanism implemented for this purpose, it shall be considered as a certified monitoring mechanism under Article 178(3) of Law 54/2024 (Article 4(4) of Regulation (EU) 2015/2020).

162. If AKEP is to establish or certify one or more monitoring mechanisms that enable end-users to determine whether there is a performance discrepancy and to obtain the results of the relevant measurements to use in certifying the performance discrepancy of their IAS, this would help to make the rights sanctioned in Articles 177-178 of Law 54/2024 more effective. The use of any certified mechanism must be at no additional cost to the end-user and must also be accessible to end-users with disabilities.

163. The methodologies that may be used by certified monitoring mechanisms are discussed further in the next section on methodology for monitoring the performance of IASs. The purpose of these guidelines on methodologies is to contribute to the consistent implementation of the provisions of Articles 177-179 of Law 54/2024 in Albania with the implementation of Articles 3-5 of Regulation (EU) 2015/2120 in EU countries.

For further clarification regarding AKEP's provision of the IAS quality monitoring mechanism to end users, see Appendix 1 this document.

Methodology for monitoring IAS performance

164. AKEP will take into account BEREC documents in implementing a measurement methodology for IAS performance, as well as in considering factors such as privacy, user environment and cross-traffic: BoR (14) 117[12] and BoR (17) 178[13].

165. When implementing the measurement methodologies, AKEP will take into account the guidelines on methodologies developed by BEREC regarding QoS in the context of Net Neutrality, in particular those contained in the following BEREC documents:

- BoR (14) 117 Monitoring quality of Internet access services in the context of net neutrality 25 September 2014;
- BoR (17) 179 Net Neutrality measurement tool specification, 5 October, 2017;
- BoR (18) 32 Annex 1 (https://etendering.ted.europa.eu/cft/cft-documents.html?cftId=3097);
- The Open Source implementation of the BEREC Net Neutrality measurement tool.

166. Based on these current guidelines, speed is calculated by the ratio of data volume to time period. Speed measurements should be made in both the download and upload directions. Speed should also be calculated based on the transport layer protocol payload. Measurements should be performed beyond the ISP leg of the end user. Details of the measurement methodology will be made transparent by AKEP.

In addition to download and upload speeds, BEREC also recommends measuring delay and jitter and the packet loss ratio.

V. Supervision and enforcement (Article 179)

Article 179(1-2) Supervision and enforcement

1. AKEP closely monitors and ensures compliance with Articles 177 and 178 of this law, and promotes the continued availability of Internet access services on a non-discriminatory basis and at quality levels that reflect advances in technology.
2. Pursuant to point 1 of this Article, AKEP may impose requirements regarding 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. AKEP shall publish annual reports regarding its monitoring and findings.

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

[13] BoR (17) 178, BEREC Net Neutrality Regulatory Assessment Methodology, https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/methodologies/7295-berec-net-neutrality-regulatory-assessment-methodology

The general approach for supervision

167. With regard to the duties and powers of AKEP set out in Article 179, there are three types of actions that AKEP can take to monitor and ensure compliance with Articles 177 and 178 of Law 54/2024.

- **Supervision**, which includes monitoring by AKEP as defined in Article 179(1), and is facilitated by the powers to collect information from ISPs under Article 179(3), in relation to:
  - Monitoring of restrictions on end-user rights (Article 177(1));
  - Monitoring contractual terms and commercial practices (Article 177(2));
  - Monitoring traffic management (Article 177(3-5));
  - Monitoring and evaluating the performance of the IAS and the impact of specialised services on the overall quality of the IAS (Article 177(7-8) and Article 178);
  - Monitoring transparency requirements for ISPs (Article 178);
- **Enforcement mechanisms,** which may include a range of interventions and the imposition of mandatory requirements/measures as set out in Article 179(1-2);
- **Reporting** by AKEP on the findings from the monitoring carried out, as defined in Article 179(2).

168. AKEP clarifies that for the actions it may take to monitor and ensure compliance with Articles 177 and 178 of Law 54/2024 referred to above, it will take into account the actions/measures taken in the EU/region countries in the framework of the implementation of Regulation EU 2015/2120, according to the BEREC Reports on the implementation of the Open Internet Regulation.

169. In order to monitor compliance, AKEP may request information from ISPs under Article 179(3) and end-users in the framework of handling complaints/resolving disputes between end-users and ISPs, or through surveys/polls.

170. Paragraphs 171-183 contain additional clarifications regarding the subsequent actions that AKEP may take.

Monitoring traffic management practices

171. AKEP will exercise the powers to collect information from ISPs on traffic management, for example by:

- assessing the traffic management practices applied by ISPs, including in exceptional cases (allowed by Article 177(5));
- requesting more complete information from ISPs regarding the practices implemented for traffic management, including:
  - a description and technical details about the affected networks, applications or services;
  - how they are affected and any other specific differentiations regarding the implementation of the practice (such as whether the practice only applies at a specific time of day or in a specific area);
  - in the case of exceptional traffic management practices going beyond those set out in Article 177(4)), a detailed justification as to why the practice is applied and the period of time for which it is applied;

- requesting data/records on implemented traffic management measures/practices;
- requesting information from ISPs related to AKEP's handling of end-user complaints/requests for dispute resolution;
- conducting assessments on potential practices resulting in restrictions on the open internet in Albania, similar to the 2012 BEREC Traffic Management Inquiry;
- collecting information and complaints received directly from end users or other information sources, such as news, blogs, forums and other discussion groups.

172. AKEP's actions may include performing technical traffic management measurements, e.g., to detect violations such as traffic congestion or restrictions. AKEP may for this purpose use commercially available instruments/tools, as appropriate and available, which enable the detection of such violations (traffic congestion and/or restrictions).

173. AKEP will implement appropriate monitoring policies to detect violations of Articles 177-178 of Law 54/2024 and determine the necessary actions to guarantee the fulfilment of the rights and obligations set forth in these articles regarding traffic management.

Monitoring and assessment of IAS performance

174. 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 its 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.

175. AKEP can use market-level assessment for the regulatory supervision envisaged by Article 179(1) to:

- cross-check that the published information is consistent with monitoring results (see paragraph 177);
- 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.

176. 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;
- assessment of the availability of different IAS offers or the range of offers offered by ISPs, as well as the level of their use by end users (in percentage);
- assessing the quality for a specific type of IAS, e.g., based on an access technology (such as DSL, cable or fibre);
- comparison of IAS offers in the market;
- investigating possible degradation caused by specialised services.

Monitoring of transparency requirements on ISPs

177. AKEP will monitor the transparency requirements (Article 178) for ISPs and may do so by:

- monitoring that ISPs have specified and published the required information according to Article 178(1);
- checking that such information is clear, accurate, relevant and comprehensible;
- cross-checking that the published information is consistent with monitoring results regarding Article 177, 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 178(2);
- collecting information on complaints related to infringements of Articles 177-178.

AKEP implementation and measures to guarantee the open internet

178. In order to ensure compliance by ISPs with the provisions of Articles 177-178 of Law 54/2024, including these Guidelines, and to promote the continued availability of IAS on a non-discriminatory basis at quality levels that reflect advances in technology, AKEP may undertake the following regulatory and supervisory measures, in accordance with its legal powers:

- To require ISPs to take corrective measures to eliminate or remove the factor/cause that is causing/creating the degradation of IAS quality;
- To impose (under Article 179(2)) requirements relating to technical characteristics in order to address breaches of open internet obligations (Articles 177-178), for example, to compel the removal or review of certain traffic management practices;
- To establish (under Article 179(2)) minimum quality of service (QoS) requirements if necessary;
- To adopt other appropriate and necessary measures (pursuant to Article 179(2)), for example those relating to the obligation of ISPs to ensure sufficient network capacity for the provision of IAS on a non-discriminatory basis of high quality;
- To request/order the cessation of violations and the taking of corrective measures within a specified deadline, combining these requests with the imposition of appropriate fines in justified cases, in accordance with Article 181 et seq. of Law 54/2024 and the relevant sub-legal acts;
- To request/order the suspension of the provision of specialised services in cases where the network capacity allocated to internet access services is not sufficient, until the ISP provides sufficient capacity for IAS, within a reasonable deadline determined by AKEP, including the imposition of appropriate fines in justified cases, in accordance with Article 181 et seq. of Law 54/2024 and the relevant sub-legal acts.
- To impose fines in cases of violations by ISPs of open internet rules, in accordance with Article 181 et seq. of Law 54/2024 and the relevant sub-legal acts.

179In the case of blocking and/or restriction, discrimination, etc., of a specific application or a specific category of applications, AKEP will require the relevant ISP to stop the restrictions of the relevant ports or restrictions of the application/applications if no valid justification/reasoning is

given for the non-compliance with Articles 177-178, in particular Article 177(5). AKEP will apply the measures under Article 179(1-2) in particular to stop practices that clearly violate the provisions of Articles 177-178. These measures may include:

- preventing blocking and/or restricting specific applications;
- prohibiting a congestion management practice that is specific to individual applications;
- the requirement that internet access performance, such as minimum or normally available speeds, be comparable to advertised/maximum speeds;
- setting quality requirements on the performance of application-specific traffic.

180. AKEP may impose binding requirements and measures on one or more ISPs, and also, in certain cases, it may be reasonable for them to be imposed on all ISPs in the market.

181. AKEP, in assessing the imposition of any of these requirements and mandatory measures, will be based on the principles of their effectiveness, necessity and proportionality:

- Effectiveness means that the requirements can be implemented by undertakings and are likely to prevent or quickly eliminate the deterioration of the IAS offer available to end-users or other infringements of Articles 177-178.
- Necessity means that, among the effective requirements or measures, the requirement/measure that is least burdensome must be chosen, i.e., the requirement/measure is decided after other regulatory means/instruments have been taken into consideration and the latter are considered insufficient, ineffective or unable to be used quickly enough to remedy the situation.
- Proportionality means limiting the requirements to the appropriate scope and that the obligation imposed by the requirement is to achieve a legitimate aim, is suitable for the purpose pursued and there is no less intrusive and equally effective alternative way of achieving that aim. For example, if certain ISPs provide degraded IAS services or violate the traffic management rules under Articles 177-178, then proportionate requirements may be focused in particular on these ISPs.

AKEP report on the open internet

182. Article 179(2) stipulates that AKEP *shall publish annual reports on their monitoring and findings*. The BEREC Guidelines for the implementation of Regulation (EU) 2015/2120 state that *the reports should be published on an annual basis, and NRAs should publish their annual reports by 30 June for the periods starting from 1 May to 30 April. The first report should be submitted by 30 June 2017, covering the period from 30 April 2016 to 30 April 2017 (the first 12 months after the implementation of the provisions).*

AKEP, taking into consideration the BEREC Guidelines as well as the deadlines for the entry into force of Law 54/2024 and the deadlines referred to in Articles 178-179 of Law 54/2024, clarifies that:

- AKEP reports on the Open Internet will be published on an annual basis by June 30, for the periods from May 1 of the previous year to April 30 of the year of publication;
- The first report on the Open Internet will be published by AKEP by June 30, 2026.;

- The publication of the Reports will be carried out on the AKEP website www.akep.al, in a section dedicated to the Open Internet.

183. In order to ensure consistent implementation of open internet rules in Albania with their implementation in EU countries, including enabling easier comparison of AKEP's annual reports on open internet with those of Regulatory Authorities of EU countries, AKEP will prepare annual reports on open internet in accordance with the BEREC Guidelines, including information, as appropriate, on the following:

- general description of the situation in Albania regarding compliance with the provisions of Articles 177-179 of Law 54/2024;
- description of monitoring activities carried out by AKEP;
- the number and types of end-user complaints and violations related to the provisions of Articles 177-179 of Law 54/2024;
- main results of the surveys conducted regarding the supervision and implementation of Articles 177-179 of Law 54/2024;
- the main results and values derived from the technical measurements and assessments carried out in relation to the supervision and implementation of Articles 177-179 of Law 54/2024;
- an assessment of the continued availability of non-discriminatory IAS at quality levels that reflect advances in technology;
- measures adopted/implemented by AKEP in accordance with Article 179(1-2).

Article 179(3) Requesting information

> 3. At the request of AKEP, providers of electronic communications to the public, including providers of internet access services, shall make available to AKEP information relating to the obligations set out in Articles 177 and 178 of this Law, in particular information relating to the management of the capacity and traffic of their network, as well as the justifications for any traffic management measures implemented. These providers shall provide the requested information in accordance with the deadlines and level of detail required by AKEP.

184. In addition to the information included in subscription contracts or made publicly available by ISPs, AKEP may request from ISPs information relevant to the obligations set out in Articles 177 and 178. The information requested by AKEP may include, among others:

- more details and clarifications regarding when, how and to which end users a traffic management practice is applied;
- justifications of any traffic management practices implemented, including whether such practices comply with the exceptions of Article 177(5) (a)-(c). In particular,
  - in relation to Article 177(5)(a), the precise legislative act, law or order on the basis of which the measure taken is implemented;
  - in relation to Article 177(5)(b), an assessment of the risk to the security and integrity of the network;
  - in relation to Article 177(5)(c), a justification/reasoning why the congestion is characterised as imminent (threatening), exceptional or temporary, together with data from previous periods relating to congestion confirming this characterisation, and the reason

why less intrusive and equally effective congestion management is not considered sufficient.

- requirements for specific services or applications that are necessary to use an application with a specific level of quality;
- information that allows AKEP to verify whether and to what extent the optimization of specialised services is objectively necessary;
- information regarding the capacity requirements of specialised services and other information that is necessary to determine whether or not sufficient capacity is available to provide specialised services in addition to any IAS provided, and the steps taken by the ISP;
- information indicating that the provision of one or all of the specialised services offered or facilitated by an ISP is not detrimental to the overall availability or quality of IAS for end users;
- details about the methodology by which speeds or other QoS parameters of the internet access service specified in subscription contracts or published by ISPs are derived;
- details of any agreements and commercial practices that may restrict the exercise of end-users' rights under Article 177(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 end-users by ISPs at customer care centres, points of sale or websites regarding their IAS;
- the number and type of end-user complaints received for a specific period;
- details about complaints received from a specific end user and the steps taken to address them.

Article 179(4) Issuing of these Guidelines

> 4. No later than 6 months after the entry into force of this law, in order to ensure the sustainable implementation of these rules, AKEP, after consulting with interested parties and based on the relevant BEREC documents, shall issue guidelines for the implementation of the obligations under this article.

185. As referred to at the beginning of this document, AKEP has prepared these Open Internet Guidelines, in accordance with point 4 of Article 179 of Law 54/2024, based on the latest BEREC Guidelines according to the document: *BEREC Guidelines on the Implementation of the Open Internet Regulation, 9 June 2022. BoR (22) 81*, making the necessary adaptations of the references of Regulation EU 2015/2120 (Articles 3-5) with the relevant references in Law 54/2024 (Articles 177-179).

Law 54/2024 entered into force on December 20, 2024. This deadline is also applicable to Articles 177-179 of Law 54/2024, except for point 3 of Article 179, which applies only to contracts concluded or renewed 1 year after the entry into force of this law and AKEP's clarifications in this Instruction.

VI. Entry into force of these Guidelines

186. This document of AKEP Guidelines for the implementation of open internet rules in Albania enters into force on the date of approval by the AKEP Board of Directors and publication on the AKEP website www.akep.al.

187. The deadlines for the start of the implementation of the provisions of Articles 177-179 of Law 54/2024 by ISPs regarding the information in subscription contracts/contractual documentation and relevant publications according to these AKEP Guidelines is 1.08.2026.

188. These Guidelines are mandatory for implementation by all undertakings who have been authorized/notified to AKEP under Law 54/2024 and the relevant sub-legal framework as internet access service providers.

APPENDIX 1: AKEP's Approach and Plan for Implementing the Open Internet Guidelines

1. Relation between the AKEP Guidelines on open internet in Albania and the BEREC Guidelines (BoR (22) 81)

The new Law 54/2024 "On electronic communications in the Republic of Albania" which entered into force on 20.12.2024, repealing Law 9918/2008, has partially approximated Directive (EU) 2018/1972 of the European Parliament and of the Council "Establishing the European Electronic Communications Code" (hereinafter EECC) into national legislation. In addition to the transposition of the EECC, Articles 177-179 of Law 54/2024 define the national framework for open internet access in Albania, which have been drafted in full compliance with Articles 3-5 of Regulation (EU) 2015/2120[14], which define the rules for open internet access mandatory to be implemented in all EU Member States.

The AKEP Guideline has been drafted in close compliance with the "BEREC Guidelines on the Implementation of the Open Internet Regulation" BoR (22) 81:

- adapting the terminology according to Albanian legislation;
- replacing the references to EU Regulation 2015/2120 (Articles 3-5) with the relevant references to Law 54/2024 (Articles 177-179) as well as the references to EECC (or other EU acts) with the relevant references to Law 54/2024 (other national acts in Albania);
- replacing the terms BEREC or NRAs with AKEP as appropriate;
- maintaining the logical structure and explanatory content of the BEREC document

The full alignment of AKEP Guidelines with BEREC aims to:

- Harmonization with European Union practices;
- Predictability and consistency for operators;
- Increasing consumer protection standards;
- Supporting Albania's European integration objectives.

Necessary clarifications/reservations

- The AKEP Guidelines do not change or replace the provisions of Law 54/2024. The Guidelines provide technical and procedural interpretation for the consistent implementation of Articles 177-179 of Law 54/2024.
- BEREC documents serve as a guiding basis, reflecting the best European experience.
- AKEP has adapted some aspects of the BEREC guidelines due to the specific local market conditions in Albania, especially in the first phase of implementation (2026-2027), taking into account the practices of EU/BEREC countries, information on which was part of the Draft Guidelines issued for public consultation.

[14] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and retail charges for regulated intra-EU communications and amending Directive 2002/22/EC and Regulation (EU) No 531/2012.

- AKEP will update these Guidelines depending on the changes/updates by BEREC of the document BoR (22) 81 on the implementation of the Open Internet Rules under Regulation (EU) 2015/2120.[15]

2. AKEP's approach and plan to implement open internet rules for some specific topics

AKEP's Guidelines will serve for the implementation of the Open Internet Rules in Albania according to Articles 178-179 of Law 54/2024. AKEP in this section presents the approach for the implementation in Albania of aspects of the Open Internet Rules related to the following 4 topics[16]:

1. Specification of *minimum, normally available and maximum internet speeds* (Article 178(1/ç));
2. Interpretation of "*significant, continuous or regularly recurring discrepancy*" between declared internet speeds and those actually experienced by subscribers/end-users (Article 178(2/d and 3));
3. Provision of a (certified) internet quality monitoring mechanism (Article 178(3)).
4. Publication of AKEP's annual reports on the open internet (Article 179 (2))

AKEP, taking into account the progress and main implementation practices in EU countries described in sections 3.1-3.3 of Annex 1 of the Draft Guidelines issued for public consultation, has determined to follow a moderate and/or self-regulatory approach for a transitional period (2026-2027) for the implementation of the rules for 3 out of the 4 issues above.

Any subsequent changes in the approaches to the 4 issues below or other issues related to the open internet will be carried out by AKEP based on the relevant public consultation procedures as defined in Law 54/2024.

2.1 Specifying minimum speed and NAS in fixed networks

AKEP has decided to follow in the first phase (2026-2027) of the implementation of the open internet rules a self-regulatory approach regarding internet speeds, where each ISP determines its own minimum and normally available speeds (NAS). Therefore, AKEP, at this stage, is not determining/specifying additional minimum obligations/requirements according to point 2 of article 179 of Law 54/2024 (which was Alternative 1 proposed in the public consultation, i.e., AKEP establishes minimum thresholds of minimum and/or NAS speed in relation to the maximum or contracted speed)

[15] The provisions of Regulation (EU) 2015/2120 on the open internet (including Articles 3-5) have recently been proposed (21.01.2026) by the EC to become part of the Digital Networks Act (DNA), which will also include the provisions of the EECC and several other EU acts (with the relevant amendments) in a single EU act/Regulation. These amendments/mergers of EU acts are still under public consultation by the EC, and do not affect the provisions of Articles 177-179 of Law 54/2024 or these AKEP Guidelines

[16] AKEP clarifies that the Guidelines document covers all issues related to the open internet, while this section focuses on the need or not to define additional rules/measures for 3 specific issues

This is an approach that allows flexibility for ISPs, as all ISPs specify their own **minimum, NAS and maximum speeds**, **as a percentage of the advertised speed /used in offers/publications (in contractual documentation).**

AKEP, taking into account the preferences and arguments of operators, including the experience in EU countries, especially in the first years of implementation of EU Regulation 2015/2120, in this final version of the Guidelines, has decided for the application of Alternative 2 of the Draft Guidelines issued for public consultation, as follows:

Every service provider offering internet access services on a fixed network includes in the subscription contracts with subscribers (the relevant contractual documentation):

- *"minimum", "normally available" and "maximum" speeds as a percentage of the declared/advertised speed (the maximum speed cannot be higher than the declared/advertised one);*
- *the relevant period(s) of the day when the subscriber's current internet access speed:*
    - *may reach "maximum speed";*
    - *is expected to be at the level of "normally available speed";*
    - *may be reduced to the "minimum speed" level.*
- *the relevant periods of the day should be expressed in time bands and/or weekdays/weekends. If terms such as "Peak"/"Off peak" time bands are used in the description of the periods, the operator shall also declare the relevant time bands (e.g., "peak" 8.00 a.m.-8.00 p.m./ off peak "8.00 pm-8.00 a.m. depending on the load conditions of its network).*

AKEP considers that this approach:

- increases transparency;
- creates realistic expectations;
- reduces the initial burden on operators but also increases incentives for competition in the qualitative aspects of Internet access service;
- prepares the ground for certified monitoring in 2027 and beyond (see below).

Mobile networks

The provisions of Article 177 (point 1/ç) as well as EU Regulation 2015/2120 (Article 4(1/d)) are more flexible regarding the requirements for access speeds in mobile networks than those in fixed networks. According to points 1 and 2 of Article 177 of Law 54/2024, AKEP in establishing minimum requirements for the quality/speed of internet access must aim to promote the continuous availability of internet access services on a non-discriminatory basis and at quality levels, reflecting advances in technology.

Based on current market conditions, AKEP does not consider imposing additional requirements for internet speeds on mobile networks (during this initial phase 2026-2027), other than those set out in Articles 177-179 of Law 54/2024 and in the Guidelines.

Informing subscribers about factors influencing the results of internet access speed measurement

AKEP, based on paragraph 164 of these Guidelines and on the document BoR (17) 178: "*BEREC Methodology for the Regulatory Assessment of Net Neutrality, 5 October 2017*", [17] clarifies that internet access service providers/undertakings have the right to include in subscription contracts with subscribers (relevant contractual documentation), information regarding factors related to the end-user environment or cross traffic that may affect the results of measurements performed by end-users/subscribers of internet access performance parameters, including internet access speeds, by network type (fixed or mobile).

Performance impact/limiting factors: fixed networks environment

- *Performance of the modem/router used (e.g., limitations of the modem/router device if not provided by the ISP)*
- *Connection type: if measurements are not performed via a wired connection (on the Ethernet port of the modem/router), but with other connections such as Wi-Fi, wireless repeaters, etc.)*
- *PC/laptop device performance (CPU and RAM load)*
- *Operating system version of the PC/laptop etc.*
- *Simultaneous use of other software such as antivirus, firewall, etc.*
- *Cross traffic: at the time of measurement, parallel traffic is generated such as data upload/download, music/video streaming, IPTV, background software updates, etc;*

Performance impact/limiting factors: Mobile Networks environment

- *Mobile device model performance;*
- *Radio connection quality*
- *Restrictions due to subscription contract (e.g., in cases of speed reduction after reaching the data limit at normal speed)*
- *Mobile device operating system version;*
- *Cross traffic (as in fixed networks above).*

In information on performance impact/limiting factors, service providers are recommended to consider the definitions/descriptions in document BoR (17) 178 (section 5.2: end-user environment)

2.2 The term "significant, continuous or regularly recurring discrepancy"

AKEP considers it reasonable for service providers to include in subscription contracts for internet access service on fixed networks the following definition and stipulations::

"Significant, continuous or regularly recurring discrepancy": *measurement results* ***over 5 (five) consecutive days*** *show that the speed received by the end-user is less than or equal to 70% of the minimum or normally available speed (NAS) specified in the subscription contract by the fixed network internet service provider.*

The service provider also stipulates in the subscription contract:

[17] BoR (17) 178, BEREC Net Neutrality Regulatory Assessment Methodology, 5 October, 2017.

1. *the deadline for reporting by the subscriber to the service provider of issues related **to significant, persistent or regularly recurring discrepancies;***
2. *the maximum deadline (no more than 30 days from reporting) for the service provider to address the issue by correcting the problem and/or providing the subscriber with proportional compensation for the relevant discrepancies;*
3. *cases where the subscriber's right to terminate the contract without early termination may be applied (e.g., failure to address the problem by the operator within the deadline set in point 2/maximum 30 days from the subscriber's reporting/complaint).*

2.3 IAS (certified) quality measurement mechanism

AKEP currently does not offer a certified mechanism for measuring the speed/quality of Internet access services (IAS), within the meaning of Article 178, point 3 of Law No. 54/2024. According to this article and in accordance with the BEREC Guidelines, the provision of such a mechanism is not mandatory for AKEP.

However, AKEP considers that a certified mechanism is essential for:
- verification of speed and quality parameters deviations;
- handling and resolving customer complaints;
- drafting the annual report on the Open Internet;
- increasing transparency and comparability in the market.

To this end, AKEP has planned to develop and make publicly available a certified IAS quality monitoring mechanism, which is expected to become operational within 2027, taking into account:
- relevant BEREC practices and guidelines;
- the experience of regulators in EU countries;
- determining the technical functionalities of the mechanism;
- relevant budget planning and procurement procedures.

Transitional phase (2026–2027)

Until the certified mechanism is put into operation, AKEP clarifies that it will follow a transitional approach, within which:
- end users/subscribers can use independent internet speed measurement tools available on the market, free of charge (e.g., OOKLA and similar);
- the results of these measurements may be used as a preliminary indication for the possible identification of performance problems and for the submission of complaints to the relevant service provider or AKEP;
- these results may serve for:
    - initiating subscriber complaints procedures and their investigation by the relevant service provider, including providing relevant solutions and/or explanations to the subscriber, which may include compensation to the subscriber for discrepancies between the declared and actual speeds;
    - escalation of the complaint/dispute to AKEP to provide a recommendation on dispute resolution, according to the provisions of Law 54/2024 and the relevant sub-legal acts;
    - AKEP's request for additional information from the relevant service provider;

- identifying potential cases of non-compliance;

However, AKEP clarifies:

- these (market) instruments do not constitute a certified mechanism within the meaning of Article 178, point 3;
- consequently, their results have no probative value for the final determination of the lack of conformity of performance, but may have value for the formal initiation/activation of the consumer's legal remedies under this provision;
- only measurements carried out in accordance with the AKEP certified mechanism, after its commissioning, will have full evidentiary value for these purposes.

2.4. Publication of AKEP periodic/annual reports regarding the open internet

In accordance with the provisions of paragraphs 182-183 of the Guidelines:

- AKEP will publish periodic reports on an annual basis regarding the Open Internet in Albania.
- Reports will be published by June 30, for the periods from May 1 of the previous year to April 30 of the year of publication.
- The publication of the Reports will be carried out on the AKEP website www.akep.al, in a section dedicated to the Open Internet.
- The first report on the Open Internet will be published by AKEP by June 30, 2026.