TRAFICOM
Liikenne- ja viestintävirasto

Checklist for Compliance with the Open Internet Regulation

Klaus Nieminen and Niko Aarnio

Traficom publications

221/2020

Table of contents

1 Foreword

The openness of the internet, or net neutrality, is guaranteed by the Open Internet Regulation[1]. In Finland, compliance with the Regulation is monitored by the Finnish Transport and Communications Agency (Traficom). The Regulation lays down provisions on the traffic management measures applied by internet access service providers (operators), specialised service provision, and the content of contractual terms. Under the Regulation, BEREC[2] has issued guidelines[3], which Traficom shall take account of in interpreting and applying the Regulation.

Pursuant to Article 3(1) of the Regulation, users of internet access services have the right to access and distribute information and content and to use and provide the applications and services of their choice, irrespective of the end-user's or provider's location or the location, origin or destination of the information, content, application or service. This principle is also called net neutrality.

End users and IASPs are still free to agree on the features of internet access services, such as speed, included data volumes or price. However, such agreements may not limit users' rights to open internet access.

Net neutrality also means that users have the freedom to use the terminal equipment (such as a mobile phone or modem) of their choice. However, the terminal equipment must meet the technical requirements specified by the operator.

In this memorandum, operators will find a list of the factors most central to their operations in light of the Open Internet Regulation and the BEREC guidelines. The checklist covers these factors on a general level, and Traficom is open to discussing new developments with relevant actors as the need for this arises.

2 Traffic Management

In accordance with the principle of net neutrality, providers of internet access services must treat all traffic equally and without discrimination, restriction or interference, irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used. Operators may thus not restrict traffic to certain internet addresses or impose restrictions on certain types of traffic, for instance.

Exceptions to the general rule regarding the equal treatment of traffic may be made in the context of reasonable traffic management (traffic classes) and specialised services as well as in the case of three specific exceptions specified in the Regulation. The Regulation also permits the provision of internet access subscriptions with different QoS levels and multiple application-agnostic QoS levels at the same time for a single subscription. All exceptions are subject to particular conditions, which are elaborated upon below.

[1] Regulation (EU) 2015/2120 of the European Parliament and of the Council laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union.
[2] BEREC is the European cooperative body of regulators for electronic communications, and Traficom takes part in its operations.
[3] BEREC Guidelines on the Implementation of the Open Internet Regulation (BoR (20) 112).

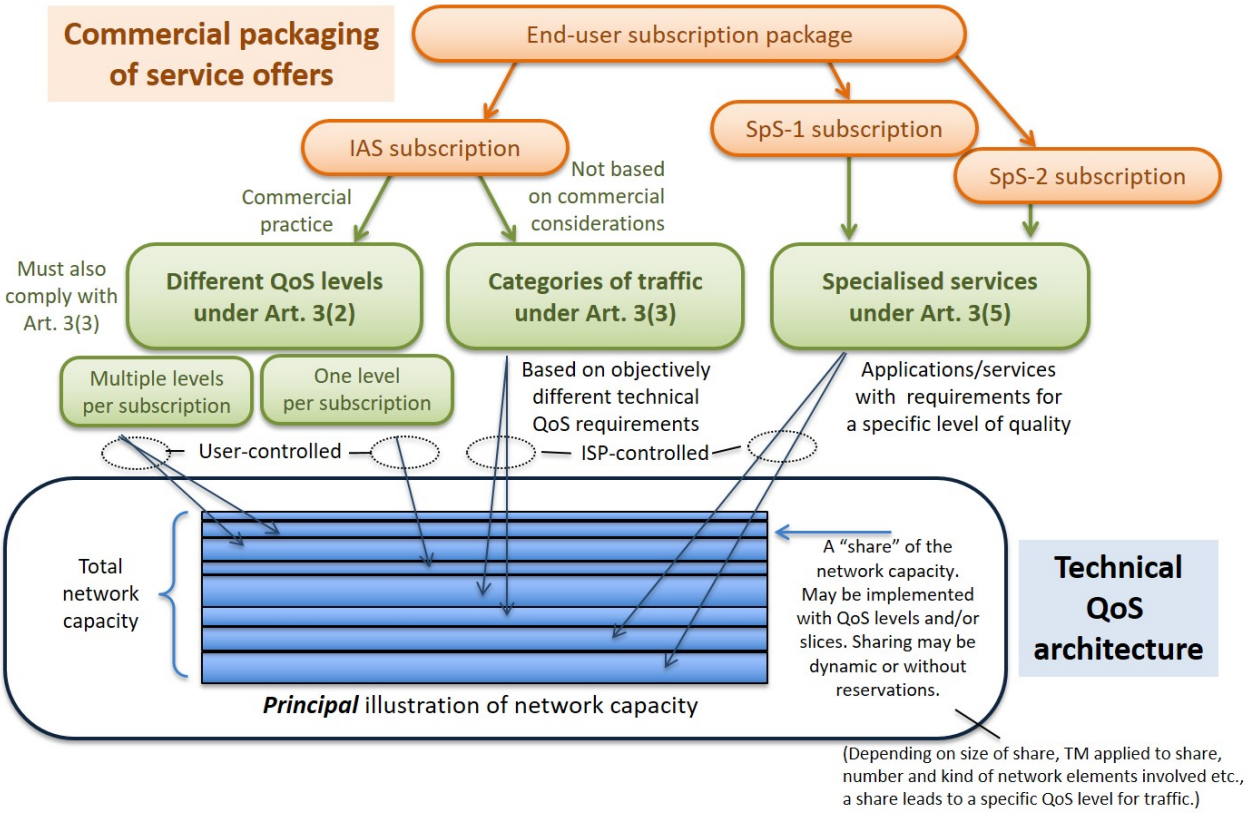

Figure 1: Framework for the provision of different QoS levels

2.1 Contractual quality levels

As stated in the BEREC Open Internet Guidelines (paragraph 53), equal treatment does not necessarily imply that all end-users will experience the same quality of service. The Regulation allows offering internet access subscriptions with different QoS levels regarding parameters like speed, latency, jitter and packet loss. Examples of such connections include broadband subscriptions offering different speeds (e.g. 100 and 300 Mbps). It is also possible to offer several connections of varying quality for the same subscription, such as low-latency connections provided on top of a broadband subscription.

In accordance with the BEREC guidelines (paragraphs 34–34d), these connections must be application agnostic, meaning that the user has the right to make decisions regarding the applications used via each connection. Furthermore, traffic management measures may not degrade the quality of other IAS subscriptions to a quality below the contract conditions. Therefore operators must also ensure that the minimum speeds promised for mobile broadband connections will be met. Contracts may not limit the rights of end-users specified in Article 3(1) of the Regulation.

In addition, operators' practices must comply with the requirements regarding the equal treatment of traffic set out in Article 3(3), subparagaph 1 of the Regulation. In accordance with recital 8 of the Regulation, comparable situations should not be treated differently and different situations should not be treated in the same way unless such treatment is objectively justified. Operators may thus employ traffic management measures to deliver different levels of quality when this is necessary in order to fulfil contractual promises made to users regarding service quality. Operators must otherwise treat all traffic equally and without discrimination, irrespective of factors including the sender. This means that mobile broadband subscriptions sold to corporations, for example, cannot be given priority over consumer subscriptions. This also applies to the subscriber connections of service operators in relation to subscriber connections provided by a network operator as a service operator.

Restricting the maximum speed of a subscription according to the agreement is permitted, as is treating subscriptions with different maximum speeds differently in the context of spectrum resource allocation.

2.1.1 Treatment of speed classes when allocating spectrum resources

Traficom has been asked to provide an interpretation of whether two internet access subscriptions with different maximum transmission speeds could be treated differently in the allocation of spectrum resources. In practice, this has concerned situations where different speed classes have been given different QCIs (quality class indicators), which means that they are given different weighting coefficients when radio resources are allocated in a base station.

This means that an operator can assign different QCI classes based on speed class, in which case the speed class differences are apparent even during regular congestion. Operators can place all subscribers in QCI class 9, in which case they are all treated in the same way. Traficom considers that in the case of mobile broadband subscriptions, operators may also use the so-called non-GBR QCI classes 6 to 9 so that the difference between the weighting coefficients given to different speed classes in the context of spectrum resource allocation is no larger than the difference between the maximum speeds of the different speed classes. In such cases, the differing treatment of the subscriptions can be considered objectively justified in accordance with the Regulation.

For example, if the weighting coefficient of a 50 Mbps subscriber connection is X, the weighting coefficient of a 100 Mbps -connection can be 2X and the weighting coefficient of a 300 Mbps connection 6X at the maximum. The difference between two weighting coefficients can also be smaller than the ratio between the transmission speeds. For example, all subscriber connections with a maximum transmission speed of ≤50 Mbps or ≤100 Mbps can be placed in the same GCI class and have the same weighting coefficient. This is necessary in order to ensure that subscriptions with slower maximum speeds continue to function during network congestion and that their speeds do not fall short of the contractually defined minimum speeds. Operators must also assess whether other measures are necessary in this context.

All subscribers belonging to the same speed class must be treated equally, i.e. the model described in this opinion cannot be applied to provide a higher quality to specific types of subscriber connections only, such as business subscriptions. This requirement of equal treatment also means that a network company must treat subscriber connections in the same speed class equally, regardless of the service operator.

As long as the above considerations are duly taken into account, the Regulation does not govern the traffic management mechanisms used, and operators may also employ the necessary traffic management measures in the core network.

2.1.2 Network slicing for different use cases

The Regulation does not prevent the construction of separate networks or the reservation of a part of a network's capacity for a particular use. It is thus also possible to productise separate network slices for different use cases.

Traficom has been asked for an interpretation regarding the possibility of reserving a certain part of the 5G network’s capacity for Fixed Wireless Access (FWA) so that the users of both the fixed and mobile broadband connections could utilise the free capacity of the other network segment. This would mean, for example, that mobile users could make use of network resources reserved for fixed connections when all of the latter's capacity is not required by fixed-connection users.

In Traficom's view, this practice should generally be allowed. However, operators must assess how these slices impact the service quality experienced by mobile users, consider their effect on service promises, and take them into account in their contractual terms.

2.2 Traffic categories

Under Article 3(3), subparagraph 2 of the Regulation, reasonable traffic management measures based on traffic categories are permitted for internet access services. The reasonable traffic management measures must be based on objectively different technical quality of service requirements of specific categories of traffic. Such requirements are typically based on latency, latency variation, packet loss, speed and particularly the specific reliability-related requirements resulting from these quality levels.

The requirements of non-discrimination, proportionality and transparency apply to traffic categories. In order for measures to be considered *non-discriminatory*, situations in which the same quality requirements apply must be treated in the same way. This also means that for example certain kinds of traffic or certain traffic categories cannot be slowed down or blocked on this basis. It does not either enable traffic category based limitations to the maximum capacity used by different applications and services.

In order for measures to be *proportionate*, they must have a legitimate aim and be suitable to achieve the aim while no less interfering and equally effective alternative ways of achieving the aim are available. Measures may also not remain applicable for longer than is necessary. *Transparency* requires that measures be described as part of the contractual terms.

Monitoring of the specific content of traffic is not permitted; the headers of the IP and transport layers can be used in traffic categorisation. The examination of the content of packets for the purposes of traffic categorisation is not permitted beyond this extent.

Traffic categories described in this section has not been widely implemented in the network and the only examples discussed have been network management traffic and a potential traffic category for real-time voice and video traffic.

2.3 Specialised services

Article 3(5) of the Regulation permits the provision of so-called specialised services. These services are not considered internet access services, and may not replace them. Article 3(5) does thus not permit the provision of broadband connections of different qualities. This is instead addressed with the help of contractual quality levels (see section 2.1).

Operators must be able to demonstrate why content, applications or services provided in this way require optimisation in order to meet the requirements of a specific level of quality. This level of quality must be specified, and it must be demonstrated that its requirements cannot be assured instead over the internet. The requirements regarding the quality of the service must be objectively necessary in order to provide the content, application or integral characteristic of the service.

Operators must also ensure that network capacity is sufficient to provide the specialised services in addition to any internet access services provided so that the provision of the former is not to the detriment of the availability or general quality of internet access services for end-users. Service quality cannot be optimised by granting general priority to optimised traffic.

Voice over LTE (VoLTE) and IPTV have typically been named as examples of services requiring optimisation. However, recent attention in this context has instead focused on machine-to-machine communications (M2M). According to the BEREC guidelines (paragraph 108a), optimisation may be considered necessary due to factors including the particular requirements of M2M/IoT devices. In such cases the devices may be resource-constrained and the provisioning of services in the network may have to deal with issues such as energy exhaustion, interference and security to maintain a specific level of quality.

2.4 Other justifiable exceptions and restricting traffic

Exceptions may also be made to the general rule of non-discriminatory traffic management as necessary and for as long as necessary in order to

a) comply with legislation, or decisions by courts or public authorities

b) preserve the security of the network and terminal equipment

c) prevent network congestion and mitigate the effects of existing congestion if it is exceptional or temporary in nature.

2.4.1 Obligations under relevant legislation

It is essential with regard to compliance with obligations under relevant legislation to ascertain that the obligation applies to the operator in question, in which case compliance can be considered necessary. The Regulation does not, however, allow for self-imposed decisions by operators on the grounds that another operator has been obliged to take certain measures, for example.

2.4.2 Maintaining information security

Traffic restrictions (e.g. port restrictions) that are not based on compliance with statutory obligations or on this information security exception may not be implemented. Any restrictions that are currently in force without a justifiable reason must also be removed.

Traficom has compiled recommendations on blocking traffic to a certain communications port for information security reasons into one Recommendation[4]. Traficom also assesses recommendations from the perspective of Open Internet Regulation, and updates its Recommendation as necessary. Restrictions not provided for in the Recommendation require particular justification. Each operator makes, however, decisions concerning the application of the recommendation independently, and is individually responsible for meeting its information security obligations. In addition, operators may be required to implement additional filters to those referred to in the recommendation.

Therefore, when considering traffic filtering in practice, it is always essential to assess whether filtering is necessary at all and if so, for how long it is necessary. As a rule, filtering measures taken for information security reasons should be temporary, and the filtering should be discontinued once the threat is removed.

Furthermore, filtering measures must be proportionate to the seriousness of the threat in question, and the filtering method that has the minimum possible impact on use must be chosen (e.g. rate limiting instead of a block).

For more detailed information on the information security obligations, see FICORA Regulation 67 on information security in telecommunications operations.

[4] Traficom Recommendation 312/2020 S: Filtering traffic in telecommunications operators' networks to certain communications ports for information security reasons.

2.4.3 Impending, exceptional or temporary network congestion

Operators may also take measures to prevent impending network congestion or mitigate the effects of exceptional or temporary congestion. Examples of situations in which exceptional measures may be taken are given in recital 15 of the Regulation. Pursuant to the Regulation, exceptional congestion should be understood as referring to unpredictable situations of congestion whose causes include a technical failure or large increases in network traffic due to emergency or other situations beyond the control of providers of internet access services.

The coronavirus pandemic was generally considered to constitute such an exceptional situation, but it did not in fact result in the kind of network congestion requiring exceptional measures referred to in the Regulation. Thus, there are virtually no practical examples of the exceptional measures provided for in the Regulation. Operators should contact Traficom if they consider it necessary to implement such measures.

As set out in recital 15 of the Regulation, the exception should not give providers of internet access services the possibility to circumvent the general prohibition on discriminating between specific traffic. Furthermore, recurrent and more long-lasting network congestion should not benefit from the exception, but should rather be tackled through the expansion of network capacity.

Measures taken on the basis of this exception are subject to ensuring the equal treatment of comparable traffic categories, and operators may thus not treat a particular service differently than other service providers in the same category.

2.4.4 Information security services sold as additional services

Under the Regulation, operators may, however, provide additional services related to information security and restricting children's use of the internet in the same way as any other content service provider. This means that if Google, for example, can provide a service over the network, the Regulation does not restrict operators' opportunity to provide a comparable service, when traffic filtering is carried out at the IP destination address determined by the terminal device. Examples of such services include HTTP proxy servers and DNS resolvers.

It is essential that the choice to use or not use such additional services not affect the features or price of the underlying internet access service. This means that users may not, for example, be offered a higher speed or lower price as a result of enabling the filtering. Users must also be able to activate and deactivate the service at their discretion. The centrally important factor with regard to interpreting the rules is whether the user him- or herself is allowed to make the decision to activate the service. Filtering services activated by default by the operator are considered to constitute part of the internet access service. For example, filtering can thus be carried out in a default DNS resolver only on the basis of the exceptions provided for in the Regulation.

3 Freedom to choose terminal equipment

Under Article 3(1) of the Open Internet Regulation, end-users have the right to use the terminal equipment of their choice. The same right is guaranteed to users under section 246, subsection 1 of the Act on Electronic Communications Services (917/2014, AECS), which states that a telecommunications operator shall not prevent a user from connecting to a public communications network any radio or telecommunications terminal equipment that meets the requirements of the Act. According to subsection 3, a subscriber must maintain equipment or a system to be connected to a public communications network in accordance with instructions from the telecommunications operator so as not to endanger the information security of the public communications network or service.

Traficom interprets these provisions to mean that, for example, a cable network operator may not restrict the cable modems allowed in its network to models it has pre-approved. Terminal equipment may, nonetheless, be subject to requirements based on the communications network's interface and characteristics, for example. If a piece of equipment compromises information security, measures can be taken in accordance with section 273 of the Act on Electronic Communications Services.

The use of terminal devices can only be restricted in accordance with the Regulation, e.g. for reasons related to information security or technical compatibility. The user's right to choose the terminal device does not apply to those devices which it is, according to an objective assessment, technically necessary to consider part of the telecommunications operator's network.

4 Terms and conditions of the contract

4.1 Information included in the contract

Contractual terms must include the information referred to in Article 4(1) of the Regulation. Operators must see to it that the terms and conditions of both currently valid and new contracts comply with the Regulation. As a general requirement, information must be presented in a clear and comprehensible manner.

The majority of the provisions laid down in the Regulation also apply to internet access services provided for corporate customers. The exceptions to this are Article 4(1), subparagaph e (description of the remedies available to the consumer) and Article 4(4) (legal effects of certified monitoring mechanisms).

4.1.1 Indicating speed and other quality parameters

Contracts must contain at least the following information about the connection speed:

- minimum, normally available and maximum speed in the case of fixed broadband;
- estimated maximum speed in the case of mobile broadband;
- and the advertised speed of the internet access service.

Traficom's Opinion on indicating the speed of internet access services supplements the information contained in the BEREC guidelines. The Opinion sets out Traficom's view regarding the reasonable method of indicating the speed of internet access service and its application in the case of high-speed subscriptions. The Opinion also provides guidance on the situations in which Fixed Wireless Access (FWA) subscriptions and hybrid subscriptions are considered fixed-network subscriptions in the context of indicating connection speed.

In addition to speed, the use of an internet access service may be impacted by other quality parameters, including latency, latency variation and packet loss. If these quality parameters may have practical effects on the use of the internet access service, information on this must be included in the contract. For example, latency in satellite broadband affects the use of applications requiring real-time data. Conversely, this information does not generally need to be provided in the case of fibre, cable and xDSL subscriptions.

An operator may not limit the fulfilment of its contractual promise regarding service quality to within its own network, because service providers are responsible for ensuring that their network capacity is sufficient. Speeds must be specified on the basis of the transport layer protocol payload. Contractual terms must also include

information on speeds after any data transfer quotas have been reached, if this entails a limitation of the speed.

4.1.2 Descriptions of traffic management measures and their effects

Descriptions of traffic management measures must include traffic management measures employed on the basis of traffic categories as well as any exceptional traffic management practices implemented in accordance with the Regulation. Descriptions must be comprehensive, and general statements of the types of traffic management measures permitted by the Regulation and used by the operator are thus not sufficient. Descriptions of the employed measures must include:

- examples of how the measures impact the user experience generally and, where necessary, as regards specific applications or services;
- an explanation as to when and how the traffic management measures are applied;
- information on traffic management measures related to the processing of personal data, i.e. which data is used and how the internet access service provider protects the data and the privacy of the service's users.

If the use of the internet access service in question is subject to a data transfer quota, the contract must describe how the size of the quota affects the user in practice and what the consequences are of exceeding the quota. It is recommended that contracts include examples of the kind of use that would lead to the quota being reached.

With regard to mobile networks, contract terms must state in a manner which is comprehensible to the user the conditions in which the maximum transmission speed is available and how congestion can affect the speeds of the different speed classes. If the operator has productised different quality levels and allocates e.g. radio resources in the manner referred to in section 2.1.1, the description must clearly state that during high load or congestion in the base station, the available speed of subscriber connections with different speed classes depends on the ratio between their maximum transmission speeds. The description must be concrete, and therefore it is recommended that the ratios between the actual weighting coefficients are mentioned at least by means of examples (for example that a 300 Mbps connection is six times faster than a 50 Mbps connection during high load situations.)

Because treating speed classes differently has a significant impact on the typical speed experienced by the user, Traficom recommends that the impacts are described by specifying the normally available speed of the subscriber connection.

Contracts must also provide information on the practical impact on the use of the internet access service of any specialised services included in the contract. If the subscription includes such IPTV services, for example, a concrete explanation must be given as to how the speed of the internet access service is affected when it is used simultaneously with the IPTV service.

4.1.3 Providing information on restrictions

If a traffic restriction permitted for a specific reason by the Regulation is considered permanent (e.g. restrictions on outgoing email traffic with regard to port 25) and the restriction may have an effect on the user of the service, such effects must be described in the contract. It is also necessary to include information on the kinds of measures the operator may take if information security is threatened.

With regard to DNS restrictions based on court rulings, it is sufficient to state in the terms of the contract that, in compliance with a court decision, access is blocked

from the service to certain websites distributing material that infringes copyright, and to include a reference to the up-to-date listing of these restrictions available online.

4.1.4 IP addresses and network address translation (NAT)

Contracts must state whether the internet access service provides IPv6 support.

If the internet access service uses NAT, the contract must state in a comprehensible manner how this may affect the use of different services via the internet access service, including using the access to provide services. The contract must clearly indicate whether NAT is used and, if the internet access service also provides IPv6 support, whether the NAT only applies to IPv4 traffic. Users must also be informed of the possibility of acquiring a public IPv4 address upon request (see also section 4.2.1).

4.1.5 Processing of complaints

Internet access service providers must adopt transparent, simple and effective procedures to process complaints from users. Complaints may concern contractual terms and conditions or a user's right to an open internet. This does not necessarily imply that separate channels must be provided for complaints, but the provider's website must supply guidance on filing complaints regarding these questions. This guidance must include information on e.g. the processing of the complaint, the channels used to contact the customer, and the authority or authorities the customer may contact in case they are unhappy with the decision of the telecommunications operator.

4.2 Contractual restrictions

Agreements between providers of internet access services and users may not limit the exercise of the rights of users (Article 3(1) of the Regulation) nor be used to deviate from the requirements regarding the non-discriminatory management of traffic (Article 3(3) of the Regulation). Contracts concluded with users may thus not be used to justify traffic management measures that violate the Open Internet Regulation or do not meet the requirements laid down in the Regulation.

This means that operators may not restrict by means of contractual terms and conditions the user's right to use the internet access service for a purpose of their choice, such as

- using or offering a particular application or service via the internet access service (e.g. using a mobile network internet access service for VoIP, peer-to-peer traffic, or file sharing)
- connecting a server to the public internet via the internet access service, including using the server as part of business activities, as long as the service is not used primarily to carry out business activities[5]
- using a mobile phone's tethering functionality, i.e. sharing the internet access service to other terminal devices
- using the terminal device chosen by the user.

An operator may not use contractual terms and conditions to restrict or reserve the right to restrict the use of any internet service via its internet access service on

[5] Under the Consumer Protection Act, a telecommunications operator is not required to provide a service used primarily for business activities on the same terms offered to consumers.

grounds other than those provided for in the Regulation. The latter include information security reasons (see section 2.4).

Furthermore, contractual terms and conditions may not be used to impose a general fair use requirement under penalty of breach of contract or to reserve a general right for the telecommunications operator to take action in relation to volumes of data transferred. Should terms and conditions of this type be included, they must be specified by e.g. indicating a precise quota for the transferred data.

4.2.1 Possibility of obtaining a public IPv4 address upon request

If NAT is used, it must be possible for the user to obtain upon request a static or dynamic public IPv4 address without separate charge. An operator can decide whether it provides dynamic, static or both dynamic and static IP addresses as described above. Users must be informed of this possibility.

This view is based on Articles 3(1) and 3(2) of the Open Internet Regulation. Under Article 3(1) of the Regulation, the end-user has, for example, the right to use and provide the applications and services of their choice via their internet access service. NAT is problematic in this light, as it clearly constitutes a practical restriction on the aforementioned right of users.

According to Article 3(2), the user rights referred to in Article 3(1) cannot be restricted by contracts or commercial practices between the parties. Because NAT in practice restricts the end-user's rights under Article 3(1) of the Regulation, Traficom considers the use of NAT a prohibited restriction. Thus, operators cannot refuse to remove such an unlawful block at the user's request or charge a fee for the operation. The requirement only extends to addresses within the current address reserve, and does not apply if the latter has been exhausted. Such address requests by users may thus not lead to a situation that may be considered unreasonably difficult for the operator.

Traficom is currently unaware of any other means to lift the restriction caused by NAT than to provide the customer with a public IPv4 address.

Opinions on the matter have also been issued in other countries, including Austria[6], Germany[7] and Croatia[8], all of which have concluded that NAT constitutes a restriction on users' rights and that operators have an obligation to offer their users the opportunity to request and obtain a public IPv4 address without a separate charge.

[6] Austria's annual net neutrality report 2020, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68270
[7] Germany's annual net neutrality report 2019, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=61112
[8] Croatia's annual net neutrality report 2019, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60728

5 Sources

Regulation (EU) 2015/2120 of the European Parliament and of the Council laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union https://eur-lex.europa.eu/eli/reg/2015/2120/oj

BEREC Guidelines on the Implementation of the Open Internet Regulation (BoR (20) 112), https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/9277-berec-guidelines-on-the-implementation-of-the-open-internet-regulation

Act on Electronic Communications Services (917/2014, AECS), https://www.finlex.fi/fi/laki/ajantasa/2014/20140917

FICORA Regulation 67 on information security in telecommunications operations, https://www.finlex.fi/data/normit/44046/M67A_2015_EN.pdf

Traficom Recommendation 312/2020 S: Filtering traffic in telecommunications operators' networks to certain communications ports for information security reasons,https://www.traficom.fi/sites/default/files/media/regulation/Suositus3122020_EN.pdf

Traficom's Opinion regarding the reasonable method of indicating the speed of internet access service, https://www.traficom.fi/sites/default/files/media/regulation/Opinion-regarding-the-reasonable-method-of-indicating-the-speed-of-internet-access-service605_923_2016.pdf

Finnish Transport and Communications Agency (Traficom)

PO box 320, FI-00059 TRAFICOM
tel. +358 29 534 5000

traficom.fi

ISBN 978-952-311-707-5
ISSN 2669-8757 (online publication)

TRAFICOM
Liikenne- ja viestintävirasto