



To BEREC  
Zigfrīda Annas Meierovica bulvāris № 14, 2nd floor  
LV-1050 Rīga  
Latvia

NN-Consultation@berec.europa.eu

Vienna, July 18th 2016

**Subject:** Public consultation on draft BEREC Guidelines on implementation of net neutrality rules

Dear Ladies and Gentlemen,

CYAN Mobile Security GmbH is a Vienna, Austria, based IT Start-up company in the field of internet security, webfiltering und nanny software (childprotection). We provide web filtering and child protection solutions based on integration at a mobile operators Mobile Internet Gateway (MIG or GGSN) as well as App solutions.

One of our costumers is T-Mobile Austria who informed us that the Austrian Regulatory Authority RTR considers our child protection solution as not compliant to the net neutrality rules according to EU Regulation 2015/2120 due to blocking internet traffic for minors (according to the decision of their parents).

For us this seems a quite strict interpretation of the EU Regulation and therefore we urge BEREC to clarify this situation in the upcoming Guidelines.

Technically, CYAN, as a third party, receives requests from the MNO gateways, checks them against our filter database and proves them against settings set up by parents for their kids. Our systems simply reply with YES or NO, but parents always have the choice to individually white- and blacklist content for their kids. Parent and kids phones are connected with help of an App to allow kids to real time ask parents for the allowance to access certain web sites or Apps – a powerful tool to strengthen the communication and education between parents and kids.

We, as an IT company, offer different set up scenarios for MNOs, like cloud-based or on-site installations. In the particular example of T-Mobile Austria, the operator has decided for an on-site installation to ensure customer data privacy – no data may leave the T-Mobile core network. CYAN strongly encourages this decision, which allows the best combination of a powerful customer solution and still strictly adhering to data privacy.

**safer  
SURFING**



CYAN Mobile Security GmbH  
A-1010 Vienna, Goldschmiedgasse 6/6-B, T. +43 1 33 66 911-0  
www.cyanmobilesecurity.com

**CYAN**  
MOBILE SECURITY

Our products and services are value add services which are offered individually to customers of MNOs. Of course in the case of child protection their parents are the buyers of our services and they will have full control of the security settings.

Of course we acknowledge BEREC's intention to harmonize the interpretation of the EU Regulation within Europe as far as possible. Our products and services are offered not only in Austria but also in other EU countries. A fragmented interpretation of the unfortunately very vague provisions of the TSM Regulation would produce high uncertainty among MNOs and especially for service offers like ours.

BEREC correctly deduces from art. 3 (2), that agreements regarding commercial and technical conditions between MNOs and end-users are allowed, as long as they do not limit the exercise of the rights of end-users laid down in art. 3(1).

In § 34 BEREC assumes that infringements of art 3 (3) "typically" restrict the exercise of end-users rights, whereas typically implies correctly, that there are important exceptions. In its consideration of art 3 (3) BEREC does not acknowledge the correct relationship between art 3 (3) and 3 (2), namely that art. 3(2) **stipulates an exception to the general rule of art 3 (3).**

On the contrary, BEREC assumes that "A practice where an MNO blocks, slows down, restricts, interferes with, degrades or discriminates access to specific content, one or more applications [or categories thereof], except when justified by reference to the exceptions of Article 3 (3) third subparagraph" would not be compatible with art. 3(3) and therefore prohibited (§ 52). BEREC therefore falsely interprets art. 3 (2) to be subordinate to art. 3 (3) and not an exception to art. 3 (3).

This would lead to absurd and contradicting results:

In practice there are several services or applications which sole purpose is to infringe art. 3 (3) in the interest of the end-user (i.e. SPAM-Filters, Anti-Virus filters, Content control for minors, etc.). These services do not restrict the exercise of end-user rights, but on the contrary amplify them. Although some of these services or applications might to some extent also be provided endpoint-based, any such service or application would always be less efficient, more cost intensive and often impossible (i.e. every device form mobile phones, to smart watches, wearables and any other "less intelligent" device would still need the full spectrum of endpoint-based protection).

An implementation of such services or applications on the level of an MNO (network level) does therefore not contradict the Regulation as long as it based on an agreement following art. 3 (2) and hence **does not contradict art. 3(1), meaning as long as the end-user has the right to end the service at any time** in order to "access and distribute information and content, use and provide applications and services, and use terminal equipment of their

**safer  
SURFING**

choice, irrespective of the end-user's or provider's location or the location, origin or destination of the information, content, application or service, via their internet access service."

The implementation of such individually agreed services and applications is not to be seen as traffic management, as traffic management is treating traffic differently.

The EC specifically (<https://ec.europa.eu/digital-single-market/en/creating-better-internet-kids>) demands to "Create a safe environment for children through age-appropriate privacy settings, **wider use of parental controls and age rating and content classification**". Our solution provides best of class protection as an integration at the MNOs GGSN/MIG, protects all devices used by kids, cannot be manipulated by minors and is under full control of their parents.


If solutions like ours will be prohibited by the net neutrality Regulation the impact of this will directly contradict important initiatives set by the EC for society at large and especially our children.

Furthermore an alternative solution developed by an European Start-up will have to be given up in the favor of App solutions offered by international OTTs. On top of that the customer will not feel any difference in its usage. The solution provided by us can be triggered and steered as well by an App or an an App like service.

**We ask BEREC to consider our comments in order to enable innovative services like ours to develop new sustainable business models and not to create unnecessary inhibitions for the safeguarding of children.**



Peter Arnoth, CEO  
CYAN Mobile Security GmbH



Nikolaus Futter, co-Founder  
CYAN Mobile Security GmbH

**safer  
SURFING**