

Available online at [www.sciencedirect.com](http://www.sciencedirect.com)

ScienceDirect

[www.compseconline.com/publications/prodclaw.htm](http://www.compseconline.com/publications/prodclaw.htm)Computer Law  
&  
Security Review

## EU update

**Kit Burden \***

DLA Piper UK LLP, London, UK

### A B S T R A C T

#### Keywords:

EU law  
Intellectual property  
Information technology law  
Telecommunications law

This is the latest edition of the DLA Piper column on developments in EU law relating to IP, IT and telecommunications. This news article summarises recent developments that are considered important for practitioners, students and academics in a wide range of information technology, e-commerce, telecommunications and intellectual property areas. It cannot be exhaustive but intends to address the important points. This is a hard copy reference guide, but links to outside web sites are included where possible. No responsibility is assumed for the accuracy of information contained in these links.

© 2016 DLA Piper UK LLP. Published by Elsevier Ltd. All rights reserved.

## 1. Telecoms

Florence Guthfreund-Roland (*Partner*) and Mathilde Hallé (*Consultant*) DLA Piper Paris

### 1.1. EUROPE: new telecom package promoting net neutrality principle adopted on 27 October 2015

On October 27th, 2015, the European Parliament adopted Regulation No. (EU) 2015/2120 “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” (the “New Regulation”).

This new so-called “Telecom Package” had been approved by the European Commission on June 30th, 2015, in a context of global revision of the current EU regulatory framework for the telecom sector (please refer to our previous post on the public consultation launched by the European Commission for the evaluation of the legal and regulatory framework for electronic communications networks and services).

Among its main innovations, the New Regulation states the principle of open internet access or “net neutrality” for the first

time under European law. It is worth noting that this principle was actually already mentioned – though indirectly – in Directive 2009/136/EC, which requires that internet users “should in any case be fully informed of any limiting conditions imposed on the use of electronic communications services by the service and/or network provider”.

The New Regulation clarifies the set of rights and obligations associated with this principle:

- End-users must have the right to access and distribute information and content, to use and provide applications and services, and to use any terminal equipment of their choice to access internet. Agreements between providers of internet access services and end-users shall not limit the exercise of these rights. Moreover, providers of internet access services must treat all types of internet traffic equally when providing internet access services.
- Providers of internet access services have the right to implement reasonable traffic management measures subject to such measures being non-discriminatory and proportionate. Nevertheless, providers can go beyond that and adopt measures to block, slow down or discriminate between specific contents, applications or services when strictly necessary, for example, to comply with EU law or to preserve the integrity and security of the network.

\* DLA Piper UK LLP, 3 Noble Street, London EC2V 7EE, UK. Tel.: +44 (0) 8700 111 111; fax: +44 (0) 20 7796 6666.  
E-mail address: [kit.burden@dlapiper.com](mailto:kit.burden@dlapiper.com)

For further information see: <http://www.dlapiper.com/>

<http://dx.doi.org/10.1016/j.clsr.2016.01.007>

0267-3649/© 2016 DLA Piper UK LLP. Published by Elsevier Ltd. All rights reserved.

- Providers of internet access services must ensure that contracts for the provision of internet access services specify several mandatory information detailing, e.g., how traffic management measures applied by the provider could impact on the quality of the services, or how any volume limitation, speed and/or other quality of service parameters may have an impact on the services. In addition, providers must put in place the procedures to address end users' complaints in relation to open internet access.
- National regulatory authorities in charge of the telecom sector have to monitor compliance with all requirements relating to the open internet access principle and can impose on any providers of electronic communications services to the public (including providers of internet access services) the additional technical requirements, including in relation to minimum quality of service requirements and/or other necessary measures. Furthermore, upon request from the national regulatory authorities, all information relevant to their obligations relating to open internet access must be made available by providers of electronic communications services.
- Member States have to lay down penalties applicable in case of violation of any open internet access related requirements.

The New Regulation, including the above requirements, will enter into force on April 30th, 2016.

To access the text of Regulation No. (EU) 2015/2120 dated October 27th, 2015 "laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union", please use the following link: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2015:310:FULL&from=EN>.

## 2. Network security

Aurelia Pons, Associate, DLA Piper Paris

### 2.1. Last steps towards the adoption of EU directive on network and information security

The European Union ("EU") took another step towards the adoption of the EU directive concerning measures for a high common level of security of network and information systems across the EU ("Directive NIS"). On 18 December 2015, the Permanent Representatives Committee ("Coreper") endorsed an informal deal struck with the EU Parliament on the compromise text of the Directive NIS presented by the Council of the EU. The procedure is expected to be concluded in spring 2016, after formal approval by the Council of the EU and the EU Parliament.

This nearly final version of the Directive NIS includes amendments made further to the understanding reached on 29 June 2015, by the Council of the EU and the EU Parliament on the main principles to be included in the Directive NIS. The Directive NIS mainly:

- lays down obligations for all member states to adopt a national NIS strategy;
- creates a cooperation group in order to support and facilitate strategic cooperation and the exchange of information among member states and develop trust and confidence amongst them;
- creates a Computer Security Incident Response Team ("CSIRTs") network in order to contribute to developing confidence and trust between member states and to promote swift and effective operational cooperation;
- establishes security and notification requirements for operators of essential services;
- establishes security and notification requirements for digital service providers; and
- lays down obligations for member states to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of networks and information systems.

One notable evolution of the draft directive is the elaboration of more detailed definitions for operators of essential services and digital services providers.

The definition of digital services now includes any online marketplace service, online search engine service, or cloud computing service, which is normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. Any entity that provides digital services is deemed to be a digital service provider.

Essential services include services provided in the sector of energy, transport, banking, financial market structures, health sector, drinking water supply and distribution and digital infrastructures (Internet exchange points, domain name system service providers and top level domain name registries). A public or private entity providing services in such sector(s) is deemed to be an operator of essential services if (i) the services provided are essential for the maintenance of critical societal and/or economic activities, (ii) the provision of such services depends on network and information systems, and (iii) an incident to the network and information systems of such services would have significant disruptive effects on their provision.

In order to avoid fragmentation in the identification of operators of essential services across member states, the directive details the criteria that should be taken into account to qualify incident having "significant disruptive effects" on the provision of the services. Additionally, an entity providing a service essential for the maintenance of critical societal and/or economic activities in several member states will be identified as operator of essential services after a consultation procedure between member states. Member states will have the obligation to review at least every two years their respective list of operators of essential services.

Both digital service providers and operators of essential services will have to:

- identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and information systems that they use with a view to ensuring continuity of the services that they provide; and

Download English Version:

<https://daneshyari.com/en/article/466381>

Download Persian Version:

<https://daneshyari.com/article/466381>

[Daneshyari.com](https://daneshyari.com)