Introduction:

- The Proposal pursues the broad objective of completing the European single market for electronic communications, in a perspective that comprises both economic and end-users stakes. The issue of 'net neutrality', or the openness of the Internet, is one of the core elements: the conditions in which communications can be filtered have already led to discussions, and to earlier positions of the EDPS.

- Account is taken of data protection issues, but the proposal does not provide for a systematic approach relating to its impact on the fundamental rights of privacy and data protection, although several measures will nevertheless have a major impact on individuals' rights. In this context, we recall that the Digital Agenda recognises the need to foster trust and confidence of users and consumers by ensuring harmonised rights inter alia for privacy and data protection.

- The comments below focus on the elements of the proposal which may affect individuals in the data protection perspective.

Consistency with data protection law:

- Article 15(4)(m) of the Proposal provides for the conditions to be met by a product to be considered as an 'Assured service quality (ASQ) connectivity product'. Among the conditions is compliance with the rules on privacy, personal data, security and integrity of networks and transparency contained in Directive 2002/21/EC and in the 'Specific Directives'. This reference is welcome as it also includes the ePrivacy Directive which provides for specific rules, including the protection of the freedom and confidentiality of communications which are to be protected in conformity with the high standards enshrined in various legal instruments at EU and national level, including some constitutional acts. It is all the more needed since the Proposal contains provisions foreseeing some possibilities of filtering of communications, even if under strict conditions.

- We suggest that this reference is complemented with a more general reference to the applicable data protection framework, which includes essential principles such as necessity and proportionality of data processing activities. These principles are core to the assessment of traffic management measures, as will be developed below. In practice, such reference should be inserted in a substantive provision. This is needed from the point of view of legal certainty, to avoid any ambiguity on the fact that the Proposals should not be considered as derogations from the data protection framework which remains fully applicable to the envisaged processing operations. We therefore recommend stating explicitly that the Proposals are without prejudice to national laws implementing Directives 95/46/EC and 2002/58/EC.

- Where reference is made to 'unsolicited communications', notably in recital 43 and Article 20, it should be clarified that this term would refer to unsolicited communications transmitted in violation of the national provisions transposing Article 13 of Directive 2002/58/EC.

- The draft Regulation provides for a definition of 'main establishment'. This definition is not identical with the definition in the proposed data protection regulation (currently in the legislative process) which determines *inter alia* the competent national supervisory authority for data protection. As both instruments would be in force together and apply to the same entities, it is necessary to ensure that the two definitions are compatible with each other in order to avoid legal uncertainty for providers as regards the competent authority and applicable legal framework.

Chapter III - rights of end users:

- We note that one of the aims of the proposal is to harmonise end-users' rights and replace related provisions of the Universal service Directive (Directive 2002/22/EC) which are "made redundant" by the Proposal (recital 66). We advise to take the opportunity that these rights are redefined here to ensure they take account of data protection rights in a more explicit way. The following comments aim at specifying users' rights accordingly.

- Net neutrality principle: The Proposal sets a principle of freedom of end users to access and distribute information or run applications and services of their choice (Article 20, as explained in recital 45). The text states that users "shall be free to agree" on the general characteristics of the services, which we support, as freedom of choice is an essential condition of a valid consent to the processing of user's data.

- While the principle of the openness of the Internet is reaffirmed, traffic management remains possible for a limited number of reasons mentioned in Article 20(2) (as explained in recital 43), including network integrity and security, exceptional network congestion, and, with the consent of the end user, protection against unsolicited communications. We support this restrictive list, as well as the requirement of consent in the case of unsolicited communications. However the Proposal does not provide sufficient precision as to the *possible methods* that may be used to manage traffic. It mentions blocking, slowing down or otherwise degrading specific services or applications, but does not specify whether deep packet inspection or other forms of monitoring of communications would be allowed and where relevant, under what conditions. In line with our opinion on net neutrality[1], we recall that:
    - it should be ensured that 'the inspection technique does not entail processing of data that is not *necessary and proportionate* vis-à-vis its intended purpose'. For instance, monitoring of IP headers may achieve the result required, in place of engaging in deep packet inspection.
    - In addition, *appropriate safeguards* should be in place, including strict limitations on the use of the data inspected and their retention, and proper information of end users.

  These requirements should be explicitly stated in Article 20 or at least in recital (43).

[1] Opinion of the European Data Protection Supervisor of 7 October 2011 on net neutrality, traffic management and the protection of privacy and personal data.

- Information to end users:

  - To ensure that consent is fully informed (as expressed in art. 20(1) last para), we suggest that details of the information listed further in Article 21 also mention privacy and data protection aspects so that there is a real choice taking into account traffic management practices and possible privacy intrusive techniques. In particular, information to end users should also contain information *about any intended traffic management measures that would allow the user to assess the degree of intrusiveness of these measures* from a privacy and data protection viewpoint and the resulting limitation of the confidentiality of communications and related traffic data, and not only from a service quality perspective, as stated article 21(1)(g), last indent, and 22(2), two last indents. This should help increase end-user confidence in their use of services, which is one of the aims of the Proposal (see in that sense recital 50). We recommend complementing Article 21 and Article 22 in that sense.

  - Article 21(6)(b) (as explained in recital 49) foresees that providers of electronic communications shall distribute information to end users on protection against risks to personal security, privacy and data 'where requested/where appropriate'. It is not clear on what basis such information would be deemed relevant or not. Unless the circumstances at stake are better defined in recital (49), we suggest deleting 'where requested' in that recital and 'where appropriate' in Article 21(6)(b). .

- National Regulatory Authorities shall ensure that traffic management measures are transparent and proportionate (Article 20(3), recital 46). They can also impose a minimum non-discriminatory quality of service. This role is particularly important, in view of the possible scope of traffic management measures, depending for instance on the interpretation of the notion of 'integrity' of the network. Imposing a minimum quality of service should also prevent that users are *forced* by the market to enter into contracts providing for traffic management they would not agree with in principle. Considering this impact in terms of data protection, we suggest that account is also taken of the competence of National *Data Protection* Authorities in this area. A paragraph could be added to Article 20(3) to provide for cooperation on aspects which are relevant from a data protection and privacy perspective. In the same spirit, we suggest that not only BEREC is consulted where necessary for the implementation of the Regulation, but also Data Protection Authorities, in the framework of the Article 29 Working Party. Recital (71) should be amended accordingly.

- Implementing powers of the Commission: Recital (70) summarises the areas in which the Commission is entrusted with implementing powers, including the safeguarding of internet access and reasonable traffic management. The Commission also has the power to adopt delegated acts, which may have an impact in a data protection perspective. This is the case in particular in Article 15(5) concerning Assured Service Quality connectivity products, concerning the respect of data protection rules (Article 15(4)(m), in connection with Annex II. The extent to which the Commission could precise data protection requirements using implementing powers is unclear. In particular, Annex II, which aims at describing the minimal parameters for ASQ connectivity products, remains quite vague in this respect. We recommend mentioning in the proposal the need for consulting the EDPS before the adoption by the Commission of any act that would have an impact on the processing of end-users' personal data.