With the reference to Guidelines on the right to the data portability (hereinafter: the „Guidelines"), Blue Media S.A. submits the following remarks and reservations to the Guidelines:

1. The right to the data portability should be reserved only for the natural persons who do not engage in business activity (i.e. consumers). Execution of right to the data portability requires spending expensive costs by service providers in order to adjust their software and IT infrastructure to the Guidelines. Computer programs and other software which is intended for business entities is also used by natural persons who engage in business (e.g. payroll software). As a result, the functionality of such software which enables the data portability (API), will have to be implemented in all kind of software, irrespective of the intended user (natural or legal person), which requires excessive costs covered by the service providers. In our opinion there is no justification for imposing such burdens on service providers in relation to entities who pursue business activity and only consumers should be entitled to the data portability.

2. According to the Guidelines (page 7), "to be within the scope of the right to data portability, data must be personal data concerning him or her, and which he or she has provided to a data controller". As a result, it is unclear whether the data provided by the third party would be covered by the right to data portability (e.g. data provided by one company to the other on the basis of the consent provided by the data subject).

3. According to the Guidelines (page 7), "in accordance with Article 20(1)(a) of the GDPR, in order to fall under the scope of data portability, processing operations must be based either on the data subject's consent (pursuant to Article 6(1)(a), or pursuant to Article 9(2)(a) when it comes to special categories of personal data) or, on a contract to which the data subject is a party pursuant to Article 6(1)(b)". It is clear that under this provision, the legal basis of personal data processing by the "current" data controller must be either "the consent" or "the contract". At the same time, the Guidelines state that "the data subject initiating the transmission of his or her data to another data controller, either gives consent to the new data controller for processing or enters into a contract with them" (page 9 of the Guidelines).

   As a result it is not clear:

   a) whether it is required that the legal basis of personal data processing by the "new" ("another") data controller is the same as with respect to the "current" data controller (i.e. the consent of the data subject or entering into the contract);
   b) whether there are only two prerequisites on which the "new" data controller is authorised to process the data received on the basis of the data portability (i.e. the "consent" or entering into the contract);
   c) if the answer to the question stated in letter b) is affirmative and the "new" data controller receives the personal data without the consent of the data subject or without the basis of "entering into the contract", what should be his next step? Should he delete the data immediately and refuse to process it?
   d) whether it is sufficient for the "current" data controller to depend only on the "technical" demand of the data subject to transfer his/her data to the "new" data controller (communicated to the "current" data controller via API) or is he required to obtain the separate and express consent of the data subject for the data transfer or his/her declaration that the data is going to be transferred in

connection with the contract concluded with the "new" data controller (e.g. accepted checkbox)?

4. According to the Guidelines, the data portability request may be provided to the "current" data controller by the data subject. Is it possible that the data subject indicates the specific destination provided by the "new" data controller to which the data should be transferred? Is it possible that the request is "technically" provided by the "new" data controller via API (on the basis of consent or conclusion of the contract with the data subject)?

5. According to the Guidelines, "a receiving data controller is responsible for ensuring that the portable data are relevant and not excessive with regard to the new data processing". The question then arises: is the "new" data controller obliged to inform the data subject that some data is considered as "not relevant" and as such it will be deleted (i.e. the "new" data controller will refuse to process it)?

6. According to the Guidelines, "current" and "new" data controllers "should implement consent mechanisms for other data subjects involved, to ease data transmission for those cases where such parties are willing to consent, e.g. because they as well want to move their data to some other data controller". In our opinion the obligation to implement such consent mechanisms would require excessive costs covered by service providers. What is more, it should be stressed, that this obligation wouldn't be appropriate with regard to some services which do not usually allow to gather contact data of third parties (e.g. bank services).

7. According to the Guidelines „the right to data portability is not a right for an individual to misuse the information in a way that could be qualified as an unfair practice or that would constitute a violation of intellectual property rights. A potential business risk cannot, however, in and of itself serve as the basis for a refusal to answer the portability request and data controllers can transfer the personal data provided by data subjects in a form that does not release information covered by trade secrets or intellectual property rights."

   As a result, it is not clear:

   a) if the data controller is obliged to assess and decide whether the data which is going to be transferred is covered by trade secrets or intellectual property rights?
   b) if the answer to the question stated in letter a) is affirmative: is the "current" data controller authorised to decide which sort of data does not infringe intellectual property rights or trade secrets and may be transferred and which is suspended?

   In our opinion the data controller ("current" and "new") should not be obliged to examine the data which is to be transferred with respect to possible infringement of trade secrets or intellectual property rights and should not be liable if such infringement arises.
8. According to the Guidelines, the "current" data controller should inform the data subject on his/her rights to data portability.

   Additional questions which arise in connecting with the above obligation:

   a) when should the data subject be informed about the right to the data portability-right after the data portability request is received by the data

controller or at the time of conclusion of the contract or expressing his/her consent to the data processing?

b) how should the data subject be informed about the right to the data portability-via email message, in the terms and conditions of the service or maybe in privacy policy?
c) the "current" data controller should inform the data subject on his/her right to the data portability before any account closure: does it mean that the data controller should retain the data for a short period of time during which the data subject could decide on transferring his/her data?

9. According to the Guidelines, the "new" data controller should provide the data subject with the complete information about the nature of personal data which are relevant for the performance of their services. The question then arises: how should the data controller provide such information-is it sufficient to send an email when the data controller receives the data portability request? Or should such information be accessible on the website for everyone?

According to the Guidelines, the "current" data controller should ensure that the data is transmitted to the proper destination. However, it should be noted that the data controller may not have any technical ability or may be not entitled to examine the security of the final destination. As a result, in our opinion, it should be explicitly stated that the "current" data controller is not liable for any acts or omissions of the "new" data controller who does not ensure the required level of data security.