EDPS formal comments on DG MARKT's public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries

The EDPS supports the Commission's initiative aimed at better defining and harmonising the conditions under which notice-and-action should take place. He however underlines that notice-and-action procedures must respect fundamental rights, including the rights to data protection and to privacy which are notably protected under Articles 7 and 8 of the Charter of Fundamental Rights of the EU, in Article 16 of the Treaty on the Functioning of the EU, and in Directive 95/46/EC and Directive 2002/58/EC.

The EDPS wishes to contribute to this public consultation by limiting his comments only to areas of the consultation that have relevance or an impact on the rights to data protection and to privacy.

I. Categories of illegal content relevant in context of N&A procedures

The EDPS is of the view that there is a need for a more pan-European harmonised definition of the notion of 'illegal content' for which the notice-and-action procedures would be applicable (**question 5**). The EDPS underlines that notice-and-action procedures may imply the processing of personal sensitive data (such as data relating to offences), which requires additional safeguards in terms of data protection (in accordance with Article 8 of Directive 95/46/EC).

Not all categories listed in question 5 carry out the same weight and would best benefit from a notice-and-action procedure being addressed to a hosting service provider (**question 24**). For instance, privacy infringements could be best reported to data protection authorities (similarly infringements of consumer protection rules could best be reported to competent authorities and/or national associations representing consumers' interests). Several types of infringements would require the involvement of law enforcement, e.g. child abuse content and terrorism related content. Furthermore, it should be defined more clearly what type of action is required from hosting service providers in those cases (for instance, define the conditions and modalities of forwarding these requests to the competent authority/body).

II. Notice and Action procedures in Europe

The EDPS agrees that there is currently too much legal fragmentation and uncertainty for hosting service providers and notice providers (**question 6**).

The EDPS supports a clarification of the notion of 'hosting' (**question 8**), taking into account the current digital environment and players. At the same time, the EDPS would like to emphasise that the definition of the activities that should be considered as 'hosting' for purpose of applying the e-commerce liability exemption regime should not affect the liability incurred by any of the service providers listed under 8) under data protection law. Many of

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

the activities considered in question 8 involve the processing of personal data of individuals, some of them relying upon or generating added value intensive personal data processing (e.g. social networks and cloud based services). In such cases, these service providers remain liable for their processing of personal data under data protection law.

Therefore, in several cases hosting service providers may be considered as data controllers under data protection law, responsible for ensuring the appropriate processing of the data. For example, in the case of social networks, the European data protection authorities have concluded that by designing the platform and the tools for the processing of personal data, social networks are controllers of the processing of personal data on their sites[1], although the content - which includes personal data - is provided by individuals[2]. As a result, social networks remain fully responsible under data protection law for the processing of personal data on their sites despite the fact that they are not the providers of the content. In a similar fashion, search engines must be considered to some extent as controllers of the personal data they process in view of the fact that they are the ones who have designed the means of the processing, i.e. the indexing and referencing tools, to perform in a certain way[3].

III. Notifying illegal content to hosting service providers

The EDPS supports the definition and implementation of EU-wide harmonised procedures and of an EU-wide harmonised form for notifying illegal content, which would help reduce national divergences and provide more legal certainty to all stakeholders.

The EDPS recommends that the procedures should take full account of the privacy and data protection principles and address issues such as:

- the confidentiality of the notice provider and of the other persons involved (e.g. complainant, suspect, witnesses, etc),
- the handling of their personal data for purpose of the assessment and afterwards (is the data retained, for how long?; is the data transmitted, to whom?),
- a transparent and easy manner to challenge a decision of a service provider to take down material, and
- the modalities of cooperation with law enforcement authorities (when, what, who).

The respect of data protection law in handling a notice is also particularly crucial in protecting alleged infringers, in particular in cases where it later appears that these persons have been subject to unjustified or abusive notices. We agree that unjustified or abusive notices should be subject to rules and possible sanctions, as those responsible for abusive notices should also be responsible under data protection rules for purposely transmitting inaccurate data (**questions 13 and 14**).

The design of the form should follow the principle of proportionality and contain only the minimum personal information required for purpose of such notification. It would be helpful if such form would contain mostly, in addition to the notice provider's contact details, questions with pre-defined multiple choice answers, and only few targeted open questions (such as 'providing a URL'). That would help ensure that only the personal data that are necessary are being processed. In this regard, we would recommend replacing the *'detailed description of the alleged illegal nature of the content*' (**question 12**) by pre-defined tick

[1] Article 29 Working Party Opinion 5/2009 on online social networking, 12 June 2009.
[2] Although individuals may also be responsible to some extent, e.g. as to the accuracy of the data, especially if their use of the social networking site goes beyond domestic use.
[3] For an analysis of the respective responsibilities, see Article 29 Working Party Opinion on data protection issues related to search engines, 4 April 2008.

boxes listing the types of possible illegal content that can be reported, amongst which a notice provider can choose.

IV. Action against illegal content by hosting service providers

The EDPS notes that there are indeed cases where law enforcement authorities need to further analyse the alleged illegal content in the context of criminal investigations and therefore removing such content may substantially limit their investigation (**Question 17**). Answer to question 17 is also linked to the classification of the type of alleged illegal content that has been notified (see our comments in point I. above). It should be further assessed whether a better classification of the types of illegal content that can be reported could be achieved, which would distinguish notices requiring involvement of other authorities/bodies (including law enforcement) from others. Separate and distinct steps could be envisaged according to the type of notice received, which may prompt hosting service providers to disable access in several cases while they would be required (preferably after a well defined review process) to remove content in specific cases.

As regards pro-active measures to be taken by hosting service providers to prevent illegal content, the EDPS underlines that it should be clarified what type of pro-active measures are being referred to (**question 22**). The EDPS emphasizes that beyond the liability exemption issue, due account must be given to Article 15 of the e-commerce Directive which clearly sets forth that service provider do not have a general obligation *'to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity*.' The Court of Justice of the EU has emphasized this principle in several cases[4]. The question may therefore arise as to whether the types of pro-active measures sought from hosting providers would be lawful under the e-commerce Directive and the e-privacy Directive and whether such measures would also be considered proportionate under the data protection Directive.

V. The role of the EU in notice-and-action procedures

The EDPS believes that the EU should play a role in contributing to the functioning of N&A procedures, preferably by providing harmonised detailed rules (at least some binding minimum rules and some binding detailed rules) (**question 23**).

Brussels, 13 September 2012

[4] See in particular Case C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, Judgement of 24 November 2011, and Case C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV*, judgment of 16 February 2012.