Opinion of the European Data Protection Supervisor

on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - "European Strategy for a Better Internet for Children"

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1],

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[2], and in particular Article 41(2) thereof,

HAS ADOPTED THE FOLLOWING OPINION

I. INTRODUCTION

I.1. Consultation of the EDPS

1. On 2 May 2012, the Commission published its Communication on a "European Strategy for a Better Internet for Children"[3] (hereafter 'the Communication').

2. Before the adoption of this Communication, the EDPS was given the opportunity to provide informal comments. The EDPS welcomes that some of his informal comments have been taken into account in the Communication. In view of the importance of the subject, the EDPS would still like to submit this opinion at his own initiative.

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.01.2001, p. 1.
[3] COM (2012) 196 final.

I.2. Objectives and background of the Communication

3. The objective of the Communication is to develop a strategy to enhance the protection of children online. The Communication is placed in the context of the EU Agenda for the Rights of the Child,[4] the Digital Agenda for Europe,[5] and the Council Conclusions on the Protection of Children in the Digital World.[6]

4. The Communication is centred on four main pillars:

   (1) stimulating quality content online for young people;

   (2) stepping up awareness and empowerment;

   (3) creating a safe environment for children online; and

   (4) fighting against sexual abuse and sexual exploitation of children.

5. The Communication outlines a number of actions to be taken by industry, the Member States and the Commission, respectively. It covers issues such as parental controls, privacy settings, age ratings, reporting tools, hotlines, and cooperation between industry, hotlines and law enforcement bodies.

I.3. Objectives and scope of the EDPS Opinion

6. The EDPS fully supports initiatives aimed at strengthening the protection of children on the Internet and at improving the means to fight against abuse of children online[7]. In two previous Opinions, the EDPS has underlined the importance of the protection and safety of children online in a data protection perspective[8]. He welcomes that this has been recognised in the Communication.

7. The growing use of the digital environment by children and the constant evolution of that environment pose new data protection and privacy risks, which are exposed in point 1.2.3 of the Communication. Such risks include, amongst others, misuse of their personal data, the unwanted dissemination of their personal profile on social networking sites, their growing use of geo-location services, their being increasingly directly subject to advertising campaigns and to serious crimes such as child abuse. These are particular risks that must be addressed in a manner appropriate to the specificity and vulnerability of the category of individuals at risk.

---

[4] EU Agenda for the Rights of the Child, COM(2011) 60 final.
[5] Digital Agenda for Europe, COM(2010) 245 final.
[6] Council Conclusions on the Protection of Children in the Digital World, 3128th EDUCATION, YOUTH, CULTURE and SPORT Council meeting Brussels, 28 and 29 November 2011.
[7] There are also a number of initiatives at international level, such as the Council of Europe Strategy for the Rights of the Child (2012-2015), CM(2011)171 final 15 February 2012.
[8] See EDPS Opinion on the Proposal for a Decision of the European Parliament and of the Council establishing a multiannual Community programme on protecting children using the Internet and other communication technologies, published in OJ C2, 7.01.2009, p. 2, and EDPS Opinion on the Proposal for a Directive on combating sexual abuse, sexual exploitation of children and child pornography, repealing framework Decision 2004/68/JHA, published in OJ C 323, 30.11.2010, p. 6.

8. The EDPS welcomes that the actions envisaged in the Communication should respect the current data protection framework (including Directive 95/46/EC and Directive 2002/58/EC[9] on e-privacy), the e-Commerce Directive 2000/31/EC[10] and the Charter of Fundamental Rights of the EU, and that it also takes into account the proposed new data protection framework[11]. The EDPS stresses that all measures to be deployed further to the Communication should be consistent with this framework.

9. This Opinion highlights the specific data protection issues that are raised by the measures foreseen in the Communication, which must be properly addressed by all the relevant addressees of the Communication, i.e. the Commission, the Member States and industry, where applicable. In particular, Chapter II underlines the specific means which can help enhance the protection and safety of children online from a data protection perspective. In Chapter III, the Opinion highlights some data protection issues that need to be addressed for the implementation of measures aimed at fighting against sexual abuse and sexual exploitation of children on the Internet, in particular concerning the use of reporting tools and the cooperation between industry, law enforcement and hotlines.

II. THE PROTECTION OF PERSONAL DATA OF CHILDREN ON THE INTERNET

II.1. Recognising reinforced rights to data protection for children online

10. The use of the Internet by children raises specific data protection issues. On the Internet, children are more vulnerable than other groups of users since they are even less equipped than others to fully understand the value of the data they disclose and the dangers that may be associated with such disclosure. Young children may not realise the consequences of their actions, or know how to manage their privacy settings. It may be difficult for them to realize that web services may be designed in a way that leads children to disclosing personal data (contact details, for example) to a wider audience than intended, with broad consequences in terms of misuse of their personal data, from behavioural targeting to cyber bullying and sexual exploitation.

11. From a legal perspective, children are considered as a specific category of individuals which deserves a particular, and reinforced, protection. Specific rights have been granted to children in several international charters and

[9] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJEU L 201, 31/07/2002, pp. 37-47.
[10] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJEU 178 L, 17/07/2000, pp. 1-16.
[11] Proposal for a Regulation of the European Parliament and Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final.

conventions[12], notably including their right to privacy[13]. From a data protection perspective, EU law does not currently set out a specific regime for children; children benefit from the general protection guaranteed in the data protection Directive 95/46/EC. However, data protection authorities in Europe have recognised the specific needs of that group of individuals and have called for the respect of their rights to privacy and data protection in a manner appropriate to their level of maturity and comprehension, and in due respect of their best interest[14].

12. Furthermore, in the proposed General Data Protection Regulation children would benefit from a specific recognition. Article 4(18) expressly defines a child as any person below the age of 18 years. The proposed Regulation foresees specific measures to ensure the effective realisation of adequate data protection for children. These measures require data controllers to provide information and communication in a language that the child can easily understand, to respect specific conditions for the processing of children's data, to implement special forms for gaining the consent for data processing, to provide them with a 'right to be forgotten' online, and to protect them from profiling[15]. The EDPS has welcomed these measures in his Opinion on the data protection reform package[16].

13. In the EU, the extent to which children can take valid action on their own, and without parental consent, with respect to the processing of their personal data is often linked to their ability to act under national civil and criminal law. The age from which children may take certain valid action on the Internet varies in Member States. To some extent, this may have been a source of legal uncertainty for organisations having children as their target audience on the Internet. These organisations have been unsure about the requirements concerning the processing of personal data of children. The proposed Data Protection Regulation has tackled the issue of age by proposing to clarify that the processing of personal data of children below the age of 13 years in the context of information society services would only be lawful if and to the extent that consent is given or authorised by their parents or custodians. *A contrario*, children above 13 years would be able to act on their own to take decisions relating to the processing of their personal data.

14. The Communication has fully embraced the importance of giving children specific and effective means to protect their personal data online, appropriate to their age group. In particular, it foresees a number of actions to be deployed

[12] See amongst others the Universal Declaration of Human Rights, the European Convention for the protection of Human Rights and Fundamental Freedoms, and the Charter of Fundamental Rights of the European Union.
[13] For example Article 16 of the UN Convention on the Rights of the Child.
[14] See Article 29 Working Party Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools), 11 February 2009, WP 160, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_en.pdf.
[15] See amongst others recitals 29, 38, 46 and Articles 6(1)(f), 6(5), 8, 11(2), 17, 33(2)(d), 38(1)(e), and 52(2).
[16] Opinion of the EDPS on the Data Protection Reform Package, 7 March 2012, OJ C 137, 12.05.2012, p. 1.

by industry to provide children with default age-appropriate privacy settings and with appropriate information before they change these settings, to recognise the specific needs of that group of individuals when engaging into online advertising with them, and to allow children to report harmful content and conduct.

15. This chapter of the Opinion focuses on pillars 2 and 3 of the Communication (as referenced in point 4 above), which envisage actions that are particularly relevant to enhancing the protection of personal data and the privacy of children. These actions aim at giving greater empowerment to children while at the same time preserving their safety while using the Internet. They include awareness raising, the deployment of an EU-wide reporting tool for children, the development of technical tools to enhance safety and privacy, and access to clear information on how to ensure that their data are protected. The EDPS analyses these actions below and makes suggestions to improve these initiatives from a data protection perspective. The reporting tool for children is analysed together with other reporting tools in chapter III.

II.2. Awareness raising

16. The EDPS welcomes the initiatives developed in sections 2.2.1 and 2.2.2 of the Communication aimed at increasing awareness. Raising children's awareness on the risks they may encounter online as well as regarding the means they may use to protect themselves is particularly crucial to enhance their protection and safety online. The EDPS underlines that since data protection is an essential component of child safety online, measures aimed at raising awareness about 'online safety' should also include information about privacy and data protection risks and rights.

17. For example, the disclosure by children of personal data on social networking sites is an issue that can have long term consequences for them as such data may be retrievable for an indefinite duration of time and may leave 'stains' on them during their adult lives. It may also have consequences for others, for example when comments or pictures are posted about other individuals. This particular risk has prompted the Commission to suggest the strengthening of the right to have data deleted into a 'right to be forgotten' online in the proposed Data Protection Regulation[17]. This right would allow individuals to ask at any time the provider of the website where the personal data were made public, to erase them and to abstain from further disseminating them. However, in practice, deleting or rectifying information that has been posted online can be a challenge and should not be seen as a solution replacing preventive action: awareness campaigns would be very helpful in making children aware of the dangers for themselves and for others of disclosing personal data (about themselves or others) on the Internet, and in allowing them to apply due care in their interaction with others and when disclosing information on the Internet. It would therefore be particularly helpful for Member States to include information and materials on data protection risks in their education curricula as well as information about how children can

[17] Article 17 of the proposed Regulation, COM(2012) 11 final.

prevent these risks by acting with caution and care, and on how to remedy those risks by the use of technical tools or the exercise of their rights.

18. Furthermore, the role of national data protection authorities is also important in the context of exchanging good data protection practices in relation to awareness raising campaigns. Data protection authorities in Europe have supported the setting up of joint initiatives regarding awareness and education of youngsters.[18] For example, the Safer Internet Day[19] which takes place every year in February has been an occasion for campaigns and competitions involving children all over Europe. Specific projects have been developed by national data protection authorities or in collaboration with them in several EU Member States, such as Portugal[20], the Czech Republic[21] and France[22], as well as EEA countries such as Norway[23]. The EDPS therefore underlines that the development of synergies between data protection authorities, national governments, the Commission and industry will be beneficial in promoting awareness on children online safety.

II.3. Age-appropriate privacy settings

19. The EDPS welcomes the initiative in section 2.3.1 of the Communication concerning the implementation by industry of technical tools to enhance the privacy of children online, in particular the development and implementation of age-appropriate default privacy settings. Embedding privacy settings by default goes along with the principle of privacy by design, which aims at considering privacy and data protection from the initial stage of the design of the processing tool. Privacy by design and the use of Privacy Enhancing Technologies has been consistently encouraged by data protection authorities, particularly as concerns processing activities targeting children.

20. A first important consideration for online service providers is to verify and delineate the extent to which children can engage in some activities online, in particular on social networking sites. In May 2010[24], the Article 29 Working Party called on private actors that have signed the 'Safer Social Networking Principles for the EU' drafted by the Commission[25] to pay specific attention to issues relating to minors, and notably the conditions to obtain the consent of their parents before they can engage in some activities online. As said, the proposed Data Protection Regulation would require parental consent to do so for children below the age of 13 years. Currently, however, there is no harmonisation of the age under which parental consent is required, and such

[18] See Resolution adopted at Prague on 29-30 April 2010 at the Spring Conference of European Data Protection and Privacy Commissioners, available at: http://www.uoou.cz/uoou.aspx?menu=125&submenu=614&loc=690.
[19] http://www.saferinternet.org/web/guest/safer-internet-day.
[20] http://dadus.cnpd.pt/.
[21] http://www.uoou.cz/uoou.aspx?loc=661.
[22] http://www.internetsanscrainte.fr/.
[23] "You decide": http://www.teknologiradet.no/FullStory.aspx?m=3&amid=4736.
[24] http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2010-others_en.htm.
[25] Safer Social Networking Principles for the EU", 10 February 2009: http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf.

consent must therefore be obtained in accordance with applicable national requirements.

21. The EDPS welcomes that specific default privacy settings should be implemented in view of the age of the child. While he considers that the strongest level of protection is required for the youngest, the EDPS nevertheless emphasizes that appropriate privacy settings should be set by default for all age ranges, and not only for the youngest. The Article 29 Working Party has underlined that basic default settings should be set forth on online social networking sites for all users, whether they are children or adults[26]. In this regard, default privacy settings for children should provide for more protective mechanisms than those that should be embedded by default for all users. For example, it would be particularly appropriate to have specific settings implemented on online social networking sites used by children, such as a tool checking the age of friends before a child can accept them, combined with settings providing for an additional check by the parents or the legal guardians of children, to validate in order to get adult friends.

Change of default settings

22. The EDPS also welcomes that industry is encouraged to provide clear information and warnings to children about the potential consequences of a change of their default settings. For such warning to be useful, it must be made clearly understandable to the minor what impact the change would have on his/her privacy and the potential harm it may cause on him/her. It may be useful for industry to develop a taxonomy to explain in a simple manner those potential harms (for example explaining what are the potential harms of being identified, being profiled, receiving cookies, etc).

23. The extent to which a child may change the default privacy settings should also be linked to the age and level of maturity of the child. It should be explored to what extent, and within which age group, parental consent would be required to validate a change of privacy settings.

Age verification

24. One difficulty in applying those default settings is the question of how service providers can determine with sufficient certainty that the individuals who are engaging on their website are within a specific age range. There are several approaches towards ascertaining the age of users, with advantages and disadvantages regarding accuracy and the scale of data collection. The least invasive way to determine the age of the individual is for this information to be voluntarily given. However, the volunteered information may not be reliable. Other models, such as full identification of the individual or systems

[26] See Article 29 Working Party Opinion 5/2009 on online social networking, p. 7: "*only a minority of users signing up to a service will make any changes to default settings. Therefore, SNS should offer privacy-friendly default settings which allow users to freely and specifically consent to any access to their profile's content that is beyond their self-selected contacts in order to reduce the risk of unlawful processing by third parties. Restricted access profiles should not be discoverable by internal search engines, including the facility to search by parameters such as age or location. Decisions to extend access may not be implicit, for example with an "opt-out" provided by the controller of the SNS.*".

designed to infer the age of the individual from his or her behaviour, aim to solve this problem, but may involve a disproportionate level of data collection and processing. While automatic systems to infer the age of a user from his or her behaviour have been suggested by researchers, there is a further danger of false identification of the age of the user under such behavioural analysis systems, particularly with respect to children who have a wide spectrum of maturity and behaviours as they grow and develop. The EDPS has noted in his Opinion on the data protection reform package that age verification tools will require that specific safeguards are taken so that only the necessary data are collected and kept.[27]

25. In this regard, the EDPS welcomes the efforts of the Commission in addressing age verification in a future EU legal framework on electronic authentication, so that website operators are able to ascertain whether the persons engaging on their site are minors, and in such case, to activate the necessary default settings. On 4 June 2012, the Commission put forward a proposal for a Regulation on electronic identification and trust services for electronic transactions in the internal market[28], which sets forth the principles and modalities of electronic authentication schemes. The EDPS emphasizes that this proposed legal framework should be fully compliant with data protection requirements and, in particular, that it should not involve the processing of more personal data than is strictly necessary for the purpose of authentication. It could allow, for instance, the age range of a person to be certified by a third party, without any details of the person being given to the website provider. The EDPS will issue an Opinion on the proposed Regulation on electronic identification and trust services, to analyse in greater details the data protection issues to be considered therein.

II.4. Providing children with clear information about the processing of their data to allow them to take informed steps

26. The Communication recommends that industry implements "contextual information" on the "privacy level" of every piece of information required or suggested to set up an online profile. The Communication does not however define what is meant by "contextual information on the privacy level of information". This can be understood as requiring service providers to inform children about the level of sensitivity of each piece of information they provide when creating an online profile. That may also require informing them about potential risks or harms they may encounter with the disclosure of such information to a restrained, larger or indefinite number of people. As described in point 22 above, it may be useful for industry to develop a common taxonomy on how to describe the level of sensitivity of each piece of information.

27. Such contextual information is welcome as it could raise more awareness on data protection at the point of collection. The EDPS, however, emphasises that it should be seen as complementary, and not as a substitute for a privacy policy that can be accessed by users when they wish to examine the privacy

[27] See footnote 16, para 321.
[28] COM(2012) 238 final.

policy of the service provider in its entirety. Service providers who act as data controllers have an obligation under data protection law, in particular as provided under Article 10 of Directive 95/46/EC, to provide detailed information to users about the processing of their data, describing in particular the processing activities they may carry out with those data (such as further using the data for profiling, data mining, etc), as well as on the rights of individuals and how they can exercise them. Furthermore, service providers acting as data controllers must ensure they respect other data protection requirements. In the proposed Data Protection Regulation, they will be held 'accountable' for such compliance with data protection law.

II.5. Advertising directed at children

28. Section 2.3.4 of the Communication describes measures to be taken to better protect children from inappropriate advertising and overspending. The EDPS welcomes the initiative in respect of online advertising to children, which requires industry to respect applicable law on online profiling and to proactively implement measures to avoid the exposure of children to inappropriate advertising in any form of online media.

29. The processing of children's personal data in the context of advertising raises two issues from a data protection perspective: it must first be ascertained whether the processing of their data for this purpose is legitimate, and where this could be the case, it must be ensured that fully adequate safeguards have been provided, or else a valid consent has been obtained for such processing.

30. In the first place, the legitimacy of advertising to children can be questioned. Because of the vulnerability of children, the collection of their personal data for direct advertising purposes may expose them to being unduly influenced by such advertising. Some data protection authorities have made it clear that any collection of data relating to minors who have not reached a sufficient maturity for marketing purposes must be considered as not being legitimate[29]. Furthermore, the practice of collecting through a minor data concerning his/her relative's habits has also been considered unfair and unlawful[30]. Having regard to this, the Article 29 Working Party has particularly emphasized that there should be no direct marketing aimed specifically at minors[31] and that data should not be collected from children with the intention to serve behavioural advertising or influence them (such as collecting data about their interests)[32]. The European Parliament has made the same

[29] See Opinion 38/2002 of the Belgian Data Protection Authority relating to the protection of the privacy of minors on the Internet, p.5: "*De façon générale, toute collecte à des fins de marketing de données relatives à des mineurs qui n'ont pas atteint l'âge de discernement doit ainsi être considérée comme non légitime. Il apparaît également déloyal et illicite de collecter via un mineur des données concernant son entourage, telles que les centres d'intérêts ou les habitudes de consommation des membres de sa famille. Il en va de même pour toute collecte de données qui serait effectuée par le truchement d'un jeu ou d'un cadeau*." The Opinion is available in French at: http://www.privacycommission.be/sites/privacycommission/files/documents/avis_38_2002.pdf.

[30] See Belgian Data Protection Authority Opinion referred to in footnote 26.

[31] See Article 29 Working Party Opinion 5/2009 on online social networking, 12 June 2009, p. 12, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf.

[32] See Article 29 Working Party Opinion 2/2010 on online behavioural advertising, 22 June 2010, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf.

demand[33]. The EDPS welcomes that the Communication has specifically tackled the issue of behavioural advertising to children, by recommending to industry that 'no such segments are created to target children'. This means that only data processing for more innocent advertising or aiming at more mature age brackets might be considered as legitimate, except where the person concerned has objected[34] or other restrictions apply.[35] This requires considerable care and self-restraint on the part of the industry.

31. Furthermore, the extent to which children can validly consent to advertising is connected to the applicable legal requirements for obtaining consent of children, which may require parental or a legal representative's consent (as described in point 13 above). Obtaining a valid consent also requires that the prescriptions of data protection law are met, namely that the consent is a freely given, specific and informed indication of the person's wishes in the sense of Article 2(h) of Directive 95/46/EC[36].

32. The EDPS takes note that the Commission Communication invites industry to build on self-regulation attempts such as the EASA Best Practice Recommendation on Online Behavioural Advertising[37]. He recalls that the Article 29 Working Party found that adherence to the current approach of this Recommendation does not result in compliance with EU data protection legislation[38]. The EDPS believes that the Commission should provide stronger encouragement to industry to develop privacy friendly self-regulatory measures at the EU-level promoting good practices with respect to online advertising to children, which should be based on full compliance with relevant legislation as the baseline.

33. In this respect, the EDPS welcomes that the Commission confirms its determination that it may look into further legislation if self-regulatory measures fail to deliver. The need to apply a reinforced level of protection for children may require taking further legislative action at EU level to ensure the appropriate consideration of children rights to privacy and data protection in the context of advertising.

---

[33] European Parliament Resolution of 15 December 2010 on the impact of advertising on consumer behaviour, available at: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2010-484

[34] Article 14 sub (b) of Directive 95/46/EC, and Article 19(2) of the proposed General Data Protection Regulation provide for a specific right to object to the processing of personal data for direct marketing.

[35] See e.g. Article 8 of Directive 95/46/EC on sensitive data, and Article 13 of Directive 2002/58/EC (e-Privacy) relating to unsolicited communications.

[36] See also Article 29 Working Party Opinion 15/2011 on the definition of consent, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf.

[37] http://www.easa-alliance.org/page.aspx/386.

[38] See Article 29 Working Party Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf.

III. DATA PROTECTION IN RELATION TO THE FIGHT AGAINST SEXUAL ABUSE AND SEXUAL EXPLOITATION OF CHILDREN

III.1. The use of reporting tools

34. The Internet has facilitated the distribution of illegal content relating to sexual abuse and sexual exploitation of children to the public at large. Furthermore, as children have become increasingly active on the Internet, it has also increased the possibilities for children to be the subject of harmful contacts or to be exposed to harmful content.

35. One way for EU policies to tackle illegal content online has been to establish, or to require industry to establish, tools by which Internet users and individuals at large can report illegal content displayed on the Internet (e.g. user generated reports on Internet websites, notice and take down policies, hotlines such as the INHOPE[39] network of hotlines)[40].

36. The Communication aims at enhancing the visibility and effectiveness of such reporting tools. Furthermore, section 2.2.3 of the Communication encourages industry to establish and deploy an EU-wide reporting tool for children, allowing them to report content and conduct that seem harmful to children across online services and devices.

37. The EDPS welcomes that the Communication clearly indicates that the initiatives foreseen to enhance notice and take down of sexually abusive material must respect the provisions of Directive 2011/92/EU[41] on combating sexual abuse and sexual exploitation of children and child pornography, the E-commerce Directive, the data protection legislation and the Charter of Fundamental Rights of the EU.

38. However, the EDPS notes that while the reporting mechanisms to be developed in the context of Directive 2011/92/EU benefit from a minimum harmonisation (in particular as to the definitions of the crimes and the modalities for their reporting), there is no such clear legal basis, nor definitions of what could be reported, in the context of the EU-wide reporting tool for children foreseen in section 2.2.3 as regards 'content and contacts that seem harmful'. The EDPS therefore recommends that the deployment of the EU-wide reporting tool for children is clearly laid down in the law.

39. Compliance with data protection requirements is particularly important for the deployment of reporting tools since these reports may involve not only the personal data of the child or the individual making the report, but also that of

[39] The International Association of Internet Hotlines. It has adopted a Code of Practice on 12 May 2010 available at:
http://www.inhope.org/Libraries/Best_Practice_Papers/Code_of_Practice_updated_2010.sflb.ashx.

[40] The Commission has outlined some of the relevant principles for reporting tools in social networking media in its document "Safer Social Networking Principles for the EU", 10 February 2009, available at: http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf.

[41] Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ L 335, 17.12.2011, p. 1–14.

the person reported as a suspect and that of possible victims. Furthermore, the data processed via these reporting tools may involve sensitive data as defined by Article 8 of Directive 95/46/EC (such as data related to suspicions of illegal activity, data concerning sex life, etc), the processing of which can only be done under strict conditions. The EDPS welcomes that the Communication underlines that reports handling should be in line with the legislation in force on data protection.

40. It must be ensured that the processing carried out through the reporting tool complies with the principle of proportionality. In this view, it is welcomed that the Commission recommends industry to develop a standard minimum reporting template 'with clear and commonly understood reporting categories' in respect of the EU-wide reporting tool for children. It would be considered good practice from a data protection perspective that such a reporting template includes pre-defined categories of crimes and/or harms to tick and that questions or comments in open fields are limited. Such a template should be designed in a way to minimise the processing of personal data to only those that are strictly necessary.

41. The development of a common reporting template in respect of other reporting tools, not only those specifically addressed to children, would also prove useful. For example, there is no common harmonised procedure in handling reports submitted through hotlines. In addition, there is a range of different privacy policies rather than a common approach. In some cases reports can be made anonymously, and in others personal and contact information is required. Where personal data is transferred, the standards of data protection may not be the same as when the information was submitted, and it may be more difficult in practice for data subjects to exercise their data protection rights if they are unaware of where their data is being processed. As a result, the handling of personal data in the context of reports made through hotlines is another area that could benefit from further cooperation at a European level towards a Code of Practice with clearer reporting procedures which reflect high standards of data protection.

42. Finally, the EDPS underlines that it could be very useful for industry to involve national data protection authorities in the development of such reporting tools to promote the development of effective reporting tools that respect data protection rules.

III.2. Cooperation between industry, hotlines and law enforcement bodies

43. The Communication foresees close cooperation between industry, hotlines and law enforcement bodies for a more effective take down of child abuse material from the Internet. Of particular concern is the lack of clarity surrounding the scope and modalities of cooperation between service providers and law enforcement authorities. It should be ensured that the modalities of such cooperation are sufficiently defined in a legal instrument that would also provide the necessary data protection guarantees.

44. The EDPS recalls that the extent to which in a legal perspective telecommunication and content service providers can be entrusted with the

tasks of reporting and blocking content that is considered illegal or harmful is questionable[42]. The EDPS emphasises that data processing activities around the investigation, reporting and prosecution of sexual abuses of children on the Internet are particularly intrusive from a data protection perspective and may only be carried out pursuant to a solid legal basis.

45. While cooperation with law enforcement is to some extent covered by the E-Commerce Directive and national legislation, other forms of cooperation, such as cooperation with the future European Cybercrime Centre[43], does not yet have a sufficiently certain basis.[44]

46. There is a need to clarify with sufficient legal certainty the modalities of the cooperation between industry, hotlines and law enforcement bodies as regards notice and take down procedures concerning child abuse material released on the Internet. In this respect, the EDPS welcomes the initiative announced by the European Commission for a horizontal measure on notice and take down mechanisms, which may allow further clarifications on the role of the various stakeholders and the modalities of their actions, within the frame of the applicable legal framework.

47. The EDPS emphasizes that such cooperation must fully respect EU law, and in particular the E-commerce Directive and the Charter of Fundamental Rights of the EU[45]. The EDPS considers that a right balance has to be found between the legitimate objective to fight against illegal content and the appropriate nature of the means used. He recalls that these tasks involve the monitoring of telecommunications, which should in principle not be executed by service providers and certainly not in a systematic way. When it is necessary in specific circumstances, it should in principle be the task of law enforcement authorities.

48. At international level, the EDPS supports the efforts of the Commission in defining a global approach to address the issues on a more coordinated and sustainable basis. The EDPS underlines that the enlargement of the scope of the INHOPE network of hotlines to countries outside the EU will require that appropriate data protection safeguards are adduced for the exchanges of personal data amongst them, in accordance with Articles 25 and 26 of Directive 95/46/EC.

[42] See EDPS Opinions referenced in footnote 8.

[43] The future European Cybercrime Centre is an initiative set out in the Communication from the European Commission to the Council and the European Parliament on the establishment of a European Cybercrime Centre, COM(2012) 140 final.

[44] There is also a lack of clarity concerning the modalities of cooperation between the European Cybercrime Centre on the one hand, and private bodies on the other. See the EDPS Opinion of 29 June 2012 on the Communication from the European Commission to the Council and the European Parliament on the establishment of a European Cybercrime Centre, available at www.edps.europa.eu.

[45] The Court has underlined the limits of the cooperation by Internet Service Providers in Case C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, Judgement of 24 November 2011 and in Case C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV*, judgment of 16 February 2012.

IV. CONCLUSION

49. The EDPS supports the Communication's initiatives to make the Internet safer for children, and in the fight against sexual abuse and sexual exploitation of children. In particular, he welcomes the recognition of data protection as a key element for ensuring the protection of children on the Internet and for empowering them to enjoy its benefits in safety.

50. The EDPS underlines that data protection requirements should be appropriately considered by industry, Member States and the Commission when implementing initiatives aimed at enhancing children's safety online, in particular:

- Member States should ensure that they include references in their education campaigns and materials to data protection risks as well as information about how children and parents can prevent them. Synergies between data protection authorities, Member States and industry should also be developed in order to foster awareness among children and parents about online safety.

- Industry should ensure that it processes personal data of children in accordance with the law, and that it obtains parental consent where necessary. It should implement default privacy settings for children which provide for more protective mechanisms than those that should be embedded by default for all users. It should also implement appropriate warning mechanisms to alert children who want to change their default privacy settings and to ensure that such a change is validated by parental consent where required. It should work on deploying appropriate tools for age verification which are not intrusive from a data protection perspective.

- In relation to information to children, industry should explore how to develop a taxonomy to provide information to children in a simple manner and to inform them about the potential risks of a change of their default settings.

- In respect of advertising to children, the EDPS recalls that there should be no direct marketing aimed specifically at young minors and that children should not be the subject of behavioural advertising. The EDPS considers that the Commission should provide stronger encouragement to industry to develop privacy friendly self-regulatory measures at the EU level, promoting good practices with respect to online advertising to children, which should be based on full compliance with data protection legislation. He also encourages the Commission to look into the possibility to further legislate at EU level to ensure the appropriate consideration of children's rights to privacy and data protection in the context of advertising.

51. The initiatives highlighted in the Communication in respect of fighting against sexual abuse and sexual exploitation of children raise a number of data protection issues, which must be carefully considered by all stakeholders in their respective field of action:

- Because of their sensitivity from a data protection perspective, the deployment of reporting tools should rely upon an appropriate legal basis. The EDPS recommends that the deployment of the EU-wide reporting tool for children foreseen in section 2.2.3 is clearly laid down in the law. He furthermore advises that is clearly defined what constitutes 'harmful conduct and content' which may be reported through the future EU-wide reporting tool for children.

- The EDPS encourages the development by industry of standard minimum reporting templates, which should be designed in a way to minimise the processing of personal data to only those that are strictly necessary.

- The procedures for reporting through hotlines could be better defined. A European Code of Practice including common reporting procedures and data protection safeguards, also in respect of the international exchanges of personal data, would improve data protection in this area.

- In order to ensure the development of reporting tools which ensure a high level of data protection, data protection authorities should be engaged in a constructive dialogue with industry and other stakeholders.

- Cooperation between industry and law enforcement as regards notice and take down procedures concerning child abuse material released on the Internet must only occur pursuant to an appropriate legal base. The modalities for such cooperation need to be more clearly defined. This is also the case concerning the cooperation between industry and a future European Cybercrime Centre.

- The EDPS considers that a right balance has to be found between the legitimate objective to fight against illegal content and the appropriate nature of the means used. He recalls that any action of surveillance of telecommunications networks, where necessary in specific cases, should be the task of law enforcement.

Done in Brussels, on 17 July 2012

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor