UDC 342.738-053.6(4-672EU) ; 341.231.14-053.6(4-672EU)

CERIF: S112, S123

Đorđe Krivokapić, PhD*

Jelena Adamović**

IMPACT OF GENERAL DATA PROTECTION REGULATION ON CHILDREN'S RIGHTS IN DIGITAL ENVIRONMENT

Raising the age of consent to data processing to 16 and allowing member states to set it at a lower age, was one of the major points of argument in the wake of passing the new EU General Data Protection Regulation (GDPR), otherwise hailed for introducing the Article 8 that recognizes children as a vulnerable group. This paper analyzes legal grounds for concerns raised over the provisions related to personal data protection of minors, possible ramifications and remedies within the given framework. It also highlights innovations and positive solutions set in the GDPR, with respect to privacy risks and opportunities for children in the information society.

Key words: *Data protection. − Privacy. − Children rights. − Information technology law. − EU law*.

1. INTRODUCTION

One of the most important novelties of the General Data Protection Regulation (GDPR),[1] which will as of 2018 replace the 1995 Directi-

* Associate Lecturer at the Faculty of Organizational Sciences, University of Belgrade, *krivokapic@fon.rs.*

** Legal Researcher at Share Foundation, *jelenaa@sharedefense.org.*

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (General Data Protection regulation), *OJ L 119, 4.5.2016*, p. 1–88, *http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf*, 21 June 2016.

ve,[2] is that it contains provisions that deal specifically with the protection of children's data. Although challenging, this is a welcome innovation. EU regulators probably did deserve criticism because 1995 Directive has been age blind. Thus, the fact that the GDPR recognized that children deserve special protection due to their vulnerability should be worthy of applause. The question if this protection is appropriate remains.

Challenge for the GDPR legislators was far from insignificant, introducing rules on protection of data of generations born in the digital age.[3] As opposed to GDPR's legislators, these children are not acquainted with other socializing environment except the one that heavily relies on the Internet. In these modern times children's "real" lives are more than ever internet concentrated. We are all in exponential speed grabbing through digital into Internet of Things (IOT) era.[4] Statistics say that an estimated one in three of all internet users in the world today is below the age of 18,[5] while one in five of all internet users in the EU is a child.[6] Thus, a common tendency that children on the Internet are observed only through the lens of the risks have to change to a more realistic approach, which includes all the opportunities on the other side of spectrum.

---

[2] 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, OJ *L 281, 23.11.1995*, p. 0031 – 0050, *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML*, last visited 21 June 2016.

[3] SMILE report: Challenges and opportunities for schools and teachers in a digital word – Lessons learned from the 2012 SMILE action research project, *http://www.eun.org/c/document_library/get_file?uuid=232671ea-32ca-4272-8b24-20328aafe8bb&groupId=43887*, 21 June 2016: "It is commonplace today to state that we are living through a digital revolution. It is a revolution that has many facets – broadband, wireless, the Cloud, big data, and many others – and one of the most potent is the emergence of social media. These new and highly social forms of media are radically different from traditional media and they are transforming whole industries as well as large swathes of our cultural, political and economic lives."; D. Frau-Meigs, L. Hibbard, "Education 3.0 and Internet Governance: A new global alliance for children and young people's sustainable digital development", *Contribution to the Global Commission on Internet Governance* 2015, *https://www.cigionline.org/publications/education-30-and-internet-governance-new-global-alliance-children-and-young-peoples-sus*, last visited 21 June 2016: "Education 3.0 addresses children's level of autonomy and empowerment on the Internet. This recognises that their online agency is higher than it is offline (i.e. starts from a younger age). Part of this response means transforming the activities of 'solo kids' online into the collective efforts of young people with advocacy skills who can both express themselves and assemble and associate, as part of the exercise of their human rights."

[4] A Brief History of Internet of Things, *http://postscapes.com/internet-of-things-history*, 21 June 2016.

[5] S. Livingstone, J. Byrne, J. Carr, "One in three: internet governance and children's rights", *The Global Commission on Internet Governance, Paper Series,* 22/2015, *https://www.cigionline.org/publications/one-three-internet-governance-and-childrens-rights*, last visited 21 June 2016.

[6] "When Free isn't", eNASCO Report, *http://www.enacso.eu/wp-content/uploads/2015/12/free-isnt.pdf*, 59, last visited 21 June 2016.

How well does the GDPR strike this balance? The answer seems to be in the cornerstone GDPR provision that regulates the age threshold for children's consent to data processing. Article 8(1) of GDPR states the following: "Where Article 6 (1)(a) applies, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 16 years, or if provided for by Member State law a lower age which shall not be below 13 years, shall only be lawful if and to the extent that such consent is given or authorised by the holder of parental responsibility over the child".

It still may be too early for a final verdict. Even though the GDPR applies directly to all EU citizens, there is some space for maneuver left to member states to sort out various potential shortcomings. According to some critics, these are many.

2. THE CRITICISM

2.1. No adequate previous analysis

Most of the criticism from practitioners in the field point out the fact that Article 8(1) went through the last minute change during a trialogue, when the threshold age was raised from 13 to 16 years, seemingly out of the blue.[7] The most questionable issue of this provision is that the respective change has been adopted with no prior stakeholder consultation and no analysis on the matter.[8]

This omission alone means that there is no obvious rationale or arguments for the adopted age threshold.[9] The result is that this core child related provision lacks legitimacy.[10] Moreover and most importantly, in

[7] Bloomberg Law: Privacy & Data Security, Data Processing Consent Age Unclear in EU Regulation, *http://www.bna.com/data-processing-consent-n57982066440/*, last visited 21 June 2016.

[8] There has been no age threshold analysis itself for GDPR purposes, but various researches have been conducted under European Commission's (EC) Safer Internet Programme with the aim to analyze various aspects of children's presence on the internet, e.g: *http://eprints.lse.ac.uk/59518/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_EU%20Kids%20Online_EU_Kids_Online_Final%20recommendations%20Sep%202014.pdf*, last visited 21 June 2016.

[9] eNASCO Report, 41–42; CHIS letter to Claude Moraes MEP, Chair of the European Parliament's LIBE Committee, *https://johnc1912.wordpress.com/2016/02/27/the-eu-gets-it-completely-wrong/*, last visited 21 June 2016.

[10] John Carr on the GDPR: Poor process, bad outcomes, *https://www.betterinternetforkids.eu/web/portal/news/detail?articleId=687465*, last visited 21 June 2016: "This is more than merely ironic because in the GDPR itself Article 33 expressly requires everyone else to carry out a data protection impact assessment which takes into account the nature, scope, context and purposes of any proposed data processing where that data processing is

the lack of any justification or underpinning principles policy makers used to set the threshold, it will be very difficult to interpret other provisions of the GDPR that aim to serve for child protection. In other words, since we do not know what the rationale behind 13 to 16 age threshold is, we cannot analyze its impact and suitability for designated purpose. The whole situation being turned upside down, now that we already have the legal provision all we can do is discuss the legal, policy and technical implications it will cause.

2.2. No definition of a "child"

The GDPR does not define "child". Age threshold set out in the Article 8(1) serves only for the purposes of that Article, i.e. for rules regarding the information society services offering. What does this mean in terms of interpreting all other provisions regulating the status and rights of the children? As all the EU member states are signatories of the UN Convention on the Rights of the Child, it seems logical to conclude that definition from that legal instrument should be used (18 years), though it would be better if this issue is explicitly sorted out by GDPR legislators. UNCRC is not mentioned anywhere in the GDPR and the EU is not a party thereto. Thus, alternatively, one may even interpret that GDPR age threshold from the Article 8(1) actually incorporates definition of the child valid for interpretation of all other provisions.

If member states should use the UNCRC definition, this would mean that the GDPR effectively has two streams of rules regarding children: all the provisions where children are mentioned would be applicable to young people aged under 18, while Article 8(1) will be an exception in its own regime. This duality of rules regarding children may potentially cause some misunderstandings and misusage of the GDPR.

2.3. No unique age threshold

The inconsistent age threshold for consent to information society services, ranging from 13 to 16 years, is controversial for at least two reasons: (i) varying threshold, which in theory could differ in each of the member states (a member state is not prevented to set its national threshold to e.g. 14 years and six months, even though this is not common and is highly unlikely) instead of one unique for all states, is directly and seriously jeopardizing one of the GDPR's most important goals – EU harmonization; (ii) there is proof serious enough that a default 16 age threshold

likely to result in a high risk for the rights and freedoms of individuals." Example of legitimate outcome: *http://blogs.lse.ac.uk/mediapolicyproject/2012/12/18/government-response-to-the-consultation-on-parental-controls-is-good-news-but-raises-new-questions/*, last visited 21 June 2016.

simply too high and sits at odds with numerous studies of child behavior on the Internet.

Regarding the first controversy and a variety of age thresholds across EU, it is evident that problems arising from conflicting laws are inevitable, for service providers as well as for regulators. Legal dilemma here is, among other situations, whether country of origin or country of destination principle will be followed. Fox example if member state 'x' has 13 years threshold, and member state 'y' has 16 years threshold, will controller from state 'x' have to respect higher threshold in country 'y'? This should be the case, otherwise country's 'y' right to set higher threshold would be futile. However, there is no clear answer in GDPR.

Due to the numbers of young internet users, this problem might be much more significant than it appears at first glance. At the moment it is expected that businesses will simply set the highest age (i.e. 16 years) by default, in order to avoid conflict of laws hustle. On the other hand, we will have to wait and see how member states would approach the matter, would they also go down the path of least resistance and adopt a default age, or would they engage more deeply in the analysis and try to make up for the lack of serious policy scrutiny on the EU level. There are concerns however that their decision might not be policy but business driven, as there is a likelihood of some powerful companies lobbying efforts to set a lower threshold in order to meet the terms of the COPPA.[11]

On the other hand, claims that 16 years is simply too high a threshold, which are strongly pointed out by a number of the experts in field,[12] have issues of their own.

2.4. Default age threshold is too high

There are serious arguments that setting the default age to 16 years actually violates children's rights under UNCRC, to which all of the

[11] John Carr on the GDPR: Poor process, bad outcomes: "Is the EU happy to contemplate or encourage the emergence of diverging youth cultures within the Union? Isn't that the obvious implication of the decision they have made? The ramifications of such a development are potentially quite profound. They should be talked about not allowed to creep in under the radar."

[12] J. Savirimuthu, "EU General Data Protection Regulation Article 8: Has Anyone Consulted the Kids?", *http://blogs.lse.ac.uk/mediapolicyproject/2016/03/01/eu-general-data-protection-regulation-article-8-has-anyone-consulted-the-kids/*, last visited 21 June 2016: "What is missing from the way policymakers have drafted Article 8 is an ability to appreciate, at a practical level, that if children as individuals are taken seriously, respect for their human rights would mean that their interests and needs are not readily assumed to be aligned with those of their parents. Also: Article 8 seems like a policy prescription attempting to address the future and does nothing more than mirror prejudices of the past." A. Pals, GDPR from a youth perspective, *https://www.betterinternetforkids.eu/web/portal/news/detail?articleId=687738*, last visited 21 June 2016.

member states are a party. Among others, UNCRC guarantees children the right to access information, to express their views and to participate in the decision-making processes, the right to learn and to develop, etc.[13] The legal rule from Article 8(1) in its effect bans children younger than 16 to actively participate in many activities on the Internet, most of which are worthy means of communication and participation, although they bear some data protection risks.[14]

In the lack of an adequate age threshold analysis, there is no way to understand how well does the adopted threshold strike the balance between data protection related risks and harms on one hand, and children's rights (UNCRC) on the other.

In the words of Sonia Livingstone, a professor at the London School of Economics and Political Science: "Even when specific provision is made for children, it focuses heavily on child protection, especially in relation to illegal activities that threaten children. This is important, for sure. But beyond this, children's rights to protection must somehow be balanced against their rights to participation, since addressing the former in isolation risks the unintended consequence of infringing the latter."[15]

The respective GDPR provision might be the result of indiscriminating between younger children and younger teenagers. A recent research indicates that a dividing line might be drawn between the children according to their school maturity,[16] and it is this differentiation that GDPR legislators appear to have ignored completely.

While it might be that younger children really do not understand the implications of their online activities and data protection risks, teen-

[13] On UNCRC rights see Young and Well Cooperative Research Centre, Melbourne 2014, *http://www.unicef.org/publications/files/Childrens_Rights_in_the_Digital_Age_A_Download_from_Children_Around_the_World_FINAL.pdf*, last visited 21 June 2016.

[14] Open letter of members of the ICT Coalition for Children Online who have been following negotiations on the GDPR, *http://www.ictcoalition.eu/news/96/GDPR%3A_parental_consent_from_age_13_to_age_16,_possibly_a_mistake*, last visited 21 June 2016; Smile report, 24: "Social media can also be used to provide an authentic audience for children's work"; A. Third *et al*., "Children's Rights in the Digital Age: A Download from Children around the World, One in three: internet governance and children's rights", *Young and Well Cooperative Research Centre*, Melbourne 2014, 5, 12, 16: "However, children's rights encompass protection, provision and participation rights, not only protection rights."; Council of Europe Explanatory Memo, *http://www.coe.int/en/web/internet-users-rights/children-and-young-people* and *https://search.coe.int/cm/Pages/result_details.aspx? ObjectID=09000016805af669*, last visited 21 June 2016.

[15] One in Three: Internet Governance and Children's Rights, *http://blogs.lse.ac.uk/mediapolicyproject/2015/11/02/one-in-three-internet-governance-and-childrens-rights/*, last visited 21 June 2016.

[16] S. Livingstone, K. Ólafsson, E. Staksrud, *Social networking, age and privacy*, EU Kids Online, London 2011, *http://eprints.lse.ac.uk/35849/*, last visited 21 June 2016

agers might be much more aware of those (even more than their parents) or might even be using the internet services to connect with their community through social networks in situations when they encounter problems and seek out the solution. Internet for teenagers is a valuable source of news and possibilities for engagement, as well as an efficient tool for engagement in civil society and environmental issues,[17] while GDPR could seriously jeopardize all those indispensable benefits.

2.5. No distinction between consent and authorization

The GDPR in Article 8(1) requires that consent is "given or authorised", but does not provide an explanation as to what is the difference between the two activities, be it material or technical. This may give a rise to doubts with regard to the nature of the parental consent, or even the moment when the consent can be given, e.g. could it be that a parent can authorize child's consent at some later point of time, after the data processing has already commenced.

This question might also be relevant in situations when a child has lied about his/her age, and the parent finds out. Can that processing be "authorized" by the parent at a later moment? Also, how should these situations be interpreted in the light of the right to objection and the right to erasure? Who would have these rights, a parent or a child, or both, and in which moment?

[17] L. Magid, "Europe Could Kick Majority of Teens Off Social Media, and That Would Be Tragic", *http://www.huffingtonpost.com/larry-magid/europe-could-kick-majorit_b_8774742.html*, last visited 21 June 2016: "Teens also use social media for engagement, not just to keep up with their friends and family (important in its own right) but to engage in civic activity. Social media is not only today's 'water cooler', but today's town square. It's the place where young people mobilize support for environmental causes, better health care, educational reform and so many other critical issues. To deny youth access to social media is to ban them from the important conversations that will shape their and our world. Nobel Peace Prize laureate Malala Yousafzai, who is now 18, started speaking publicly about the rights of women and girls in Pakistan and other countries long before she turned 16. Under this regulation, she could have been prevented from speaking out without her parents' consent. [...] Given what's happening in the world today, we need more youth communicating and participating, not fewer. Although we have heard reports about a tiny number of people who may be using social media to radicalize youth, the fact is that there are a very large number of people using social media for positive counter-speech and to mobilize young people in every country and among every ethnic and religious group to seek peaceful solutions to our problems." Also: World Summit on the Information Society, Geneva Declaration of Principles and Plan of Action, principle 11, *http://www.itu.int/net/wsis/documents/doc_multi.asp?lang=en&id=1161|1160*, last visited 21 June 2016: "We are committed to realizing our common vision of the Information Society for ourselves and for future generations. We recognize that young people are the future workforce and leading creators and earliest adopters of ICTs. They must therefore be empowered as learners, developers, contributors, entrepreneurs and decision-makers. We must focus especially on young people who have not yet been able to benefit fully from the opportunities provided by ICTs. We are also committed to ensuring that the development of ICT applications and operation of services respects the rights of children as well as their protection and well-being."

A guidance on these matters would be more that useful.

2.6. "Holder of parental responsibility" as the only consent giver

The Article 8(1) is drafted very narrowly in terms of who can give consent on behalf of the child. The GDPR gives this right only to the parents or the holders of parental responsibility. However, one may ask why the legislators did not take into account a possibility of introducing certain competences in this respect also to qualified persons that are engaged in schools and education?[18]

There is a number of reasons why some parents would simply not be able to fulfill the role designated for them in the GDPR.

It may easily be conceived that a number of parents or holders of parental responsibility across the EU do not possess enough knowledge, experience or computer skills to exercise this right. On the other hand, information society services have already found their valuable use in various classrooms, by skilled educators. These activities can now be at risk of losing their effectiveness, because parents have to be involved. In other words: "The added layer of bureaucracy required to procure parental permission before any teacher could use information society tools in class would undermine any possibility of schools fulfilling this role, and at the same time stop the valuable flow of guidance that young people are able to take home to parents and siblings".[19]

Parents may also refuse to give consent due to their own lack of understanding as to how information society services function, what their goals are, what the risks and threats are, and most importantly from the GDPR perspective, how their use could put their children's and their families' personal data at risk. Unfortunately, there has been no research regarding the computers skills and literacy among parents across the EU in all the areas that are relevant for their performance of this rather important task envisaged for them in the GDPR.

Finally, the GDPR legislators regrettably did not pay necessary attention to the real life situations when parental responsibility is not performed in the child's best interest. Such parents might as well intentionally misuse their rights and prevent their children from engaging with people who might be of assistance to them through information society

[18] Examples of use of social media in education can be found in Smile Report, 25; also Council of Europe Explanatory memo in its point 3 states that internet safety responsibilities are vested with "teachers, educators and parents", *http://www.coe.int/en/web/internet-users-rights/children-and-young-people-explanatory-memo*, last visited 21 June 2016.

[19] J. Richardson et al., Letter of concern to the draft General Data Protection Regulation, *http://www.antibullyingpro.com/blog/2015/12/11/letter-expressing-concern-to-the-draft-general-data-protection-regulation-13to16*, last visited 21 June 2016.

services, while there are proofs that endangered children tend to reach out for help using these tools.[20] Exception provided in the GDPR preamble regarding preventive or counselling services offered directly to a child, does not seem to address this issue with enough necessary clarity.

All these reasons are concisely summed up by Larry Magid: "Some parents may not have the literacy or technology skills to fill out the necessary consent mechanisms, others may be afraid to provide information that they fear might get into the hands of government or immigration authorities, many will simply be confused by the consent mechanisms, some may be too busy or too preoccupied with the challenges of providing for their families. There will be many parents who will refuse to give consent because they don't want to support their children's curiosity in such areas as religion, civic engagement or sexual health or orientation. And, sadly, there are some parents who abuse or mistreat their children who may want to keep them from being able to reach out for help".[21]

Therefore, since we are now left with narrow wording of Article 8(1), the focus should turn to the education of parents. Due to the pace at which digital age has familiarized Internet with everyday lives of people, internet education for children is likely to be more detailed and substantive than the one their parents receive. Thus, it might be that some children are more IT literate than their parents.[22] There is a research indicating that children possesses more experience then their educators particularly in the field of social media.[23] But since it is the parents who should give the consent, their IT literacy should be at an appropriate level. The question is: does the EU bear responsibility in bringing forward this issue, and if yes, how it should be implemented?

2.7. Other issues

Practitioners in the field have raised certain additional questions regarding the interpretation of the Article 8(1). Namely, Martin Sloan and

[20] J. Richardson et al.: "Sadly, we know that some parents do not always act in their child's best interests. The Internet can represent a lifeline for children to get the help they need when they are suffering from abuse, living with relatives who are addicted to drugs or alcohol, or seeking confidential LGBT support services, to name a few. Although the proposed recital 29 makes an exception for direct counselling services, we know that peer support through media platforms often plays a positive role for young people under physical or mental duress"; also in D. Frau-Meigs, L. Hibbard, 22.

[21] L. Magid, Europe Could Kick Majority of Teens Off Social Media, and That Would Be Tragic.

[22] Recommendation Rec(2006)12 of the Committee of Ministers to member states on empowering children in the new information and communications environment, *https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805af669*, last visited 21 June 2016.

[23] Smile report, 38.

Kathryn Alexander have asked: "It is also unclear whether any form of materiality test will apply. For example, if information is only being collected using cookies will parental consent be required? Or is it only where a particular level/type of information is being collected? Given the multitude of devices and browsers that people use to access information society services, technically managing the consent process will be particularly difficult if the user can access the service without creating a user account".[24]

Even though the GDPR in paragraph 3 of the Article 8 declares: "Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child", member states might experience difficulties in harmonizing their contractual laws with GDPR Article 8(1). And some of them, e.g. United Kingdom, would definitely have to adapt their practice regarding use of information society services in order to meet Article 8(1) requirements.

3. ON THE BRIGHT SIDE

3.1. Pioneering legislation focused on privacy

The fact that children's rights and need for their special protection are explicitly acknowledged in the GDPR, and that the GDPR in its various provisions recognizes that children are a group of users that deserve particular protection, is in essence a major step forward.[25] The GDPR also openly acknowledges the children's special position and their needs in online environment through a special reference in the preamble, which reads: "Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child".[26]

It has been widely acknowledged that the safety of children on the Internet is a major concern, but before GDPR there has been no legislation whatsoever on the European level that regulated this matter directly.

[24] M. Sloan, K. Alexander, GDPR and the Digital Age of Consent for Online Services, *http://www.scl.org/site.aspx?i=ed46357*, last visited 21 June 2016.

[25] G. González Fuster, "GDPR: we all need to work at it!", *https://www.betterinternetforkids.eu/web/portal/news/detail?articleId=694148*, last visited 21 June 2016.

[26] See items 58, 65, 71, 75 of GDPR preamble.

Regarding the balance of the risks and opportunities stemming from information society services, there are opinions that children's right to privacy (which of course includes their personal data) is at the moment in such need for protection that it should come before other rights. [27] Some research also show evidence that children aged under 16 do not understand information services privacy issues[28] or legal protection available to them.[29]

The threats for children on the Internet are real and unavoidable.[30] Research shows that dangers stem from practice of many information service providers, while on the other hand there are positive examples of privacy non-invasive practices that can be used as role models.[31]

Therefore, what should be explored in more detail is whether children's rights can still be exercised and expressed through other online means. In other words, the question that deserves special attention in assessing the GDPR's impact on children of certain age is: could the same opportunities that are available through information society services be obtained (online or offline) through certain less invasive and harmful tools with regards to data protection?

It should be pointed out that the GDPR is a piece of legislation that primarily deals with privacy (data protection) and not safety in general,

[27] A. Keen, "Free speech shouldn't be more important than the safety of our children", *http://thenextweb.com/insider/2016/02/06/free-speech-shouldnt-be-more-important-than-the-safety-of-our-children/*, last visited 21 June 2016: "The challenges involved with implementing these kinds of measures do not negate the need to make the internet a safer place for its youngest users. We protect children when they need protecting, not when it's 'feasible'."

[28] S. Livingstone, K. Ólafsson, E. Staksrud, 7.

[29] A. Third *et al*, 49, 74: "Evidence generated by this project overwhelmingly showed that children's greater levels of access to digital media does not imply a greater awareness of their rights in the digital age. Rather, if we are to support children to better realise their rights using digital media, then this will require a concerted effort. To date, it appears that children are not necessarily being given the opportunities to consider how digital media might positively impact their rights, although it is clear that most children have a clearer conception of how digital media might infringe on their rights in the digital age."

[30] EU Kids Online, Findings, Methods and Recommendations, *http://eprints.lse.ac.uk/60512/1/EU%20Kids%20onlinie%20III%20.pdf*, last visited 21 June 2016.

[31] J. Morton, Hacked off, *http://www.toynews-online.biz/opinion/read/hacked-off/045915*, last visited 21 June 2016; 2015 GPEN Sweep – Children's Privacy, *http://194.242.234.211/documents/10160/0/GPEN+Privacy+Sweep+2015.pdf*, last visited 21 June 2016: "Many websites and apps targeted at, or popular among, children are collecting personal information without offering kids and their parents adequate protective controls to limit the use and disclosure of such personal information, or a simple means of deleting an account permanently. That said, one third of websites or apps that were swept demonstrated that they could be successful, appealing and dynamic without the need to collect any personal information at all."

though the critics seem to pay little attention to the difference. Some research imply that children are not concerned with their privacy issues by default when they engage in online activities, on the contrary.[32] Therefore, when conducting analysis of the purpose of GDPR Article 8(1) implications, focus should be placed on data protection related risks, which is only one segment of the online safety risks.

3.2. Clear language adapted to children

The GDPR sets a requirement that any information and communication, when processing is addressed to a child, should be articulated in such a clear and plain language that the child can easily understand it. This principle of transparency aimed particularly at the children is important because of the manner in which children access Internet, that is mostly when they are alone, but also because of the availability of the devices that have internet access (e.g. children's personal phones and tablets).

It remains yet to be seen how the transparency principle would actually be implemented, but given the fact that thus far controllers tended to conceal what they do with the data they collect, a direct pressure to them to reveal their practices should lead to improvements in this respect. With regards to the children, it should lead to a change in perception where children are not treated like just another group of prospective consumers, but a vulnerable group of internet users.[33] Particular spotlight on nature of their consent to data processing seems on one of the big steps forward.[34]

3.3. Indirect influence of GDPR novelties to children

There is a number of GDPR provisions that have generally improved European data protection regime when compared to the 1995 Directive, which indirectly but significantly benefit the children.

---

[32] S. Livingstone, K. Ólafsson, E. Staksrud, 18; see also: D. Smahel, M. F. Wright, "Meaning of online problematic situations for children. Results of qualitative cross-cultural investigation in nine European countries", *EU Kids Online, London School of Economics and Political Science*, *http://www.ijvs.org/files/EUKIDSONLINE-June-2014.pdf*, last visited 21 June 2016.

[33] D. Frau-Meigs, L. Hibbard, 21: "As ever younger children access the Internet, the corporate sector has a vested interest in lowering the age barriers of Internet consent (from 13 down to eight), and uses the access to education argument for lobbying purposes. The sector is effectively not treating young people online as children but as consumers (and even prescribers to their parents), whose uses attract a lot of attention in marketing research."

[34] Linklaters, "The General Data Protection Regulation: A survival guide", *http://www.linklaters.com/pdfs/mkt/london/TMT_DATA_Protection_Survival_Guide_Singles.pdf*, last visited 5 September 2016.

One of those is the broadening of the personal data definition, setting a clearly what personal data include (e.g. clear reference to metadata). Such "widening" of the personal data definition is even more significant because of the increase in number of "things" that collect data, including children's data. In addition to a potential complexity of personal data notion for young people, it might be that they experience even more difficulties in understanding of the Internet of Things concept, and the risks arising therefrom.[35]

The GDPR has also set higher standards for consent quality and has narrowed possibilities for controllers to rely on legitimate interest justification. Profiling of personal data is also stricter now when compared to 1995 Directive. In addition to increased obligations of controllers, the GDPR is also setting certain obligations to processors. Commission's powers are widened, in terms of territorial scope of the GDPR application, and in terms of opportunity to impose significant fines.

New rights of data subjects and obligations of controllers and processors introduced by the GDPR also benefit protection of children's data, e.g. privacy by design and privacy by default, data portability, data protection impact assessments etc. In this respect, right to be forgotten i.e. right to erasure is particularly important from children's perspective.

Article 17 of the GDPR particularly states that one of the grounds for data erasure request is when "the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)". Such a provision has incorporated position of Council of Europe on this topic, which is stated in the Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet.[36]

In regards to the implementation of the right to be forgotten, the final provision of the Article 17(2) imposes the obligation of the controller that has received erasure request to take reasonable steps to inform other controllers about the erasure request by such controllers of any links to, or copy or replication of those personal data, "taking account of available technology and the cost of implementation", but it does not mention data processors. This could pose a risk that the right to be forgotten cannot be fully implemented.

[35] On ethical aspects of Internet of Things see: G. Baldini, M. Botterman, R. Neisse, M. Tallacchini, "Ethical Design in the Internet of Things", *Science and Engineering Ethics*, 2016, *http://link.springer.com/article/10.1007%2Fs11948-016-9754-5*, last visited 21 June 2016.

[36] Council of Europe Explanatory memo, point 5; also Council of Europe, Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet, *https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805d3d2d*, last visited 21 June 2016.

Finally, even though the GDPR does not explicitly clarify, it should be understood that the right to be erased can be used (i) by children whose data is collected on the basis of their parent's consent, when they reach age above prescribed 13–16 threshold, as well as (ii) by parents whose children lied about their age in order to freely use information society services, if they find out about this before a child reaches the required age threshold.

3.4. Incentive to create privacy friendly business models

As already noted, the GDPR's accent is on data protection. Since the information service providers have shown little care for data protection and privacy issues, especially when children are involved, a change was inevitable at some point. Now that strict rules of the GDPR are in place, business models will have to adapt to this new business environment.

Although one may claim (e.g. the US companies) that children related provision of the GDPR will in practice be the obstacle to innovation, it can also be argued that the current state of affairs favored unproportionally business to detriment of privacy, and that the balance should be restored.[37]

4. CONCLUSION

Although the negotiations of the GDPR were a perfect opportunity to dedicate much more time and energy to get an optimally balanced legal provision regarding the use of information society services by children, it seems that for the moment nothing more could be done on the EU level. In this sense, one possible angle of looking at the 13–16 age range could be that it did leave a necessary maneuver space for member states to take this matter further and make more sensible national legislation. This will of course require additional efforts of all stakeholders, but member states could use the mentioned criticism as guiding tools for making the improvements in national legislation.[38]

---

[37] B. Dainow, "Understanding the new EU data regulations", *http://www.imediaconnection.com/article/195098/understanding-the-new-eu-data-regulations*, last visited 21 June 2016.

[38] M. Schmalzried, "GDPR: A 'flexible' step in the right direction", *https://www.betterinternetforkids.eu/web/portal/news/detail?articleId=687553*, 21 June 2016; see also, E. Lievens, Ending the shifting game: towards true responsibility for children's rights in the digital age, *http://www.lse.ac.uk/media@lse/events/pdf/IAMCR16/Lievens.pdf*, last visited 5 September 2016.

Thus, it will have to be the member states who will balance privacy risks and information society service related opportunities for children aged between 13 and 16. The level of their IT education, when compared to level of their parents' knowledge and experience, should be inevitable part of the balancing result. However, regardless of the actual legislative results, we can conclude that in order for any legal rule to have its intended effect, continued educational efforts of both children and parents seem to be the key to efficient data protection practices across the EU.[39]

REFERENCES

Baldini, G., Botterman, M., Neisse, R.,Tallacchini, M., "Ethical Design in the Internet of Things", *Science and Engineering Ethics* 2016.

Cumbley, R., Van Overstraeten, R., Pauly, D., "The General Data Protection Regulation: A survival guide", Linklaters.

Frau-Meigs, D., Hibbard, L., "Education 3.0 and Internet Governance: A new global alliance for children and young people's sustainable digital development*", Contribution to the Global Commission on Internet Governance* 2015.

Livingstone, S., Byrne, J., Carr, J., "One in three: internet governance and children's rights", *The Global Commission on Internet Governance Paper Series* 22/2015.

Livingstone, S., Ólafsson, K., Staksrud, E., "Social networking, age and privacy", EU Kids Online, London 2011.

Nairn, A., Carr, J., Lilliu, B., "When Free isn't", eNASCO, Rome 2016.

O' Mahony, D. *et al*., "SMILE report: Challenges and opportunities for schools and teachers in a digital word – Lessons learned from the 2012 SMILE action research project", SMILE 2012.

O'Neill, B., Staksrud E., with members of the EU Kids Online network, "Final recommendations for policy", *EU Kids Online & LSE*, September 2014.

[39] D. Frau-Meigs, L. Hibbard, 2: "Children and young people are increasingly reliant on the Internet for their everyday lives. They communicate, share and collaborate online. They use it to learn and play. They recognise its importance for their adult working lives. Considering their increasing access, agency and autonomy in using content and services, their protection as a vulnerable group needs to be coupled with their education as emerging citizens to ensure they develop a healthy and positive relationship regarding the Internet. Their general well-being, participation in society, and prospects of employment greatly depend on Media and Information Literacy (MIL) as the new set of basic skills for the 21st century, where computational thinking interfaces with the rich and diverse 'cultures of information' (news, data, documents, codes, etc.)."

Smahel, D., Wright, M. F., "Meaning of online problematic situations for children. Results of qualitative cross-cultural investigation in nine European countries", *EU Kids Online* 2014.

Third, A., *et al*., *Children's Rights in the Digital Age: A Download from Children Around the World*, Young and Well Cooperative Research Centre, Melbourne, 2014.

Article history:
Received: 13. 9. 2016.
Accepted: 28. 11. 2016.