Routledge
Taylor & Francis Group

Information & Communications Technology Law

ISSN: 1360-0834 (Print) 1469-8404 (Online) Journal homepage: https://www.tandfonline.com/loi/cict20

Consent for processing children's personal data in the EU: following in US footsteps?

Milda Macenaite & Eleni Kosta

To cite this article: Milda Macenaite & Eleni Kosta (2017) Consent for processing children's personal data in the EU: following in US footsteps?, Information & Communications Technology Law, 26:2, 146-197, DOI: 10.1080/13600834.2017.1321096

To link to this article: https://doi.org/10.1080/13600834.2017.1321096

Published online: 10 May 2017.

INFORMATION & COMMUNICATIONS TECHNOLOGY LAW, 2017
VOL. 26, NO. 2, 146–197
https://doi.org/10.1080/13600834.2017.1321096

Routledge
Taylor & Francis Group

Consent for processing children's personal data in the EU: following in US footsteps?

Milda Macenaite and Eleni Kosta

Tilburg Institute for Law, Technology and Society (TILT), Tilburg University, Tilburg, Netherlands

ABSTRACT

With the recent adoption of the General Data Protection Regulation (GDPR), the European Union (EU) assigned a prominent role to parental consent in order to protect the personal data of minors online. For the first time, the GDPR requires parental consent before information society service providers can process the personal data of children under 16 years of age. This provision is new for Europe and faces many interpretation and implementation challenges, but not for the US, which adopted detailed rules for the operators that collect personal information from children under the Children's Online Privacy Protection Act (COPPA) almost two decades ago. The article critically assesses the provisions of the GDPR related to the consent of minors, and makes a comparative analysis with the requirements stipulated in the COPPA in order to identify pitfalls and lessons to be learnt before the new rules in the EU become applicable.

KEYWORDS

Children; consent; data protection; General Data Protection Regulation; COPPA

1. Introduction

Children are actively present online at an ever-younger age. It is estimated, that globally one in three internet users are under the age of 18.[1] Online, children not only enjoy exciting opportunities of playing, creating, learning, self-expressing, experimenting with relationships and identities, but are also disclosing increasing amounts of their personal data. Ubiquitous computing and the increasing datafication of everything[2] is seen as enhancing online privacy risks, such as commercial exploitation and misuse of personal data, profiling, identity theft, the loss of reputation and discrimination. For example, as the consequence of dataveillance practices via wearable and mobile devices, social media platforms, and educational software, 'children are configured as algorithmic assemblages […] with the possibility that their complexities, potentialities and opportunities may be circumscribed'.[3] In addition, due to their particular behavioural

CONTACT Milda Macenaite m.macenaite@uvt.nl

[1]Sonia Livingstone, John Carr and Jasmina Byrne, 'One in Three: Internet Governance and Children's Rights' (2015) Global Commission on Internet Governance Paper Series No. 22.

[2]Viktor Mayer-Schönberger and Kenneth Neil Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Houghton Mifflin Harcourt, 2013).

[3]Deborah Lupton and Ben Williamson, 'The Datafied Child: The Dataveillance of Children and Implications for Their Rights' (2017) 19(5) New Media & Society 780, 787.

characteristics, emotional volatility and impulsiveness, children (especially teenagers) are seen as being more vulnerable in comparison to adults online.[4] Developmental psychology provides evidence that adolescents can be more active and risk-prone online.[5] They may be less capable of evaluating perilous situations and can be more easily misled, given their lack of awareness vis-à-vis the long-term consequences of their virtual actions.[6] These specific developmental features of children might be easily exploited by online marketers who collect personal data and employ special techniques such as 'real-time bidding, location targeting (especially when the user is near a point of purchase), and "dynamic creative" ads tailored to their individual profile and behavioral patterns'.[7]

Empirical studies show that privacy risks are common on the internet[8] and privacy concerns constitute one of the main worries among children in Europe.[9] In the same vein, adults widely support the introduction of the special data protection measures for children. According to an Eurobarometer survey, 95% of Europeans believed that 'underage children should be specially protected from the collection and disclosure of personal data' and 96% thought that 'minors should be warned of the consequences of collecting and disclosing personal data'.[10]

Given these online risks and public concerns, there have been increasing calls from policy-makers and academics to transform children's rights, in particular the rights guaranteed by the UN Convention on the Rights of the Child (UN CRC), to cater for the 'digital age'.[11] Among the rights to provision and participation, the UN CRC recognises

[4]Judith Bessant, 'Hard Wired for Risk: Neurological Science, "the Adolescent Brain" and Developmental Theory' (2008) 11(3) Journal of Youth Studies 347, 358 (criticises research on adolescent brain as 'it begins with a prejudice ("they" are "different" "irrational" and "deficient") and then threatens to expand the civil and social disadvantages that already severely affect too many of our young people'. Bessant claims that 'some young people are sometimes at risk not because their brains are different, but because they have not had the experience or opportunity to develop the skills and judgment that engagement in those activities and experiences supply'.)

[5]Andrew Hope, 'Risk-Taking, Boundary-Performance and Intentional School Internet "Misuse"' (2007) 28(1) Discourse: Studies in the Cultural Politics of Education 87.

[6]Jay N Giedd, 'The Teen Brain: Insights from Neuroimaging' (2008) 42(4) Journal of Adolescent Health 335; Elizabeth R McAnarney, 'Adolescent Brain Development: Forging New Links?' (2008) 42(4) Journal of Adolescent Health 321; Tim McCreanor and others, 'Consuming identities: Alcohol marketing and the commodification of youth experience' (2009) 13 (6) Addiction Research & Theory 579; Laurence Steinberg, 'Risk Taking in Adolescence: New Perspectives from Brain and Behavioral Science' (2007) 16 (2) Current Directions in Psychological Science 55; Laurence Steinberg, 'Social Neuroscience Perspective on Adolescent Risk-Taking' (2008) 28(1) Developmental Review 78.

[7]Kathryn C Montgomery, 'Youth and Surveillance in the Facebook Era' (2015) 39(9) Telecommunications Policy 771; Kathryn C Montgomery and Jeff Chester, 'Data Protection for Youth in the Digital Age: Developing a Rights-Based Global Framework' (2015)1(4) European Data Protection Law Review 291.

[8]For example, according to the empirical data of the EU Kids online, 9% of children aged 11–16 in Europe have experienced personal data misuse online. See Sonia Livingstone and others, 'Risks and Safety on the Internet: The Perspective of European Children' (LSE, EU Kids Online, London 2011).

[9]Giovanna Mascheroni and Kjartan Ólafsson, *Net Children Go Mobile: Risks and Opportunities* (2nd edn Educatt, Milan 2014)

[10]European Commission, 'Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union' (June 2011) <http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf> 196 and 203.

[11]Council of Europe, Strategy for the Rights of the Child (2016–2021) (March 2016); UN Committee on the Rights of the Child, Report of the 2014 Day of General Discussion 'Digital Media and Children's Rights' (May 2015); UNICEF, 'Privacy, Protection of Personal Information and Reputation Rights' (2017) Discussion paper <https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf> accessed 5 April 2017; UK Children's Commissioner, 'Growing Up Digital: A Report of the Growing Up Digital Taskforce' (January 2017) 19(5): 657 <http://www.childrenscommissioner.gov.uk/sites/default/files/publications/Growing%20Up%20Digital%20Taskforce%20Report%20January%202017_0.pdf> accessed 9 April 2017; UK House of Lords Committee on Communications, 'Growing up with the Internet' (2nd Report of Session 2016–17) (March 2017) <https://www.publications.parliament.uk/pa/ld201617/ldselect/ldcomuni/130/130.pdf> accessed 9 April 2017; Sonia Livingstone and Amanda Third, 'Children and Young People's Rights in the Digital Age: An Emerging Agenda' (2017) 19(5) New Media & Society 657; Sonia Livingstone and Brian O'Neill, 'Children's Rights Online: Challenges, Dilemmas and Emerging Directions' in Simone van der Hof,

children's rights to protection, including a specific protection against arbitrary or unlawful interference with children's privacy, and unlawful attacks on their honour and reputation (Article 16).[12]

Yet, protection of informational privacy in the European Union (EU) has been designed for 'everyone', conflating adults and children in one single group of data subjects. Since 1995, minors are covered by the age-generic data protection provisions provided by Directive 95/46/EC with no special focus on the processing of children's data. The newly adopted EU General Data Protection Regulation (2016/679)[13] (hereinafter 'GDPR' or 'Regulation') has significantly changed the *status quo* and rejected the 'age-blind' approach to data subjects. The GDPR, which has faced long debates during its adoption process,[14] explicitly recognises that children need more protection than adults. As explained by Recital 38 of the GDPR, children merit special protection as they 'may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data', especially online. To provide such special protection, the GDPR has introduced far-reaching changes in relation to the processing of minor's personal data online, such as child-appropriate information, a stricter right to erasure, and stronger protection against marketing and profiling.[15] Most importantly and controversially, in cases when the processing of personal data of children takes place on the basis of consent (in accordance with Article 6(1)(a) GDPR), Article 8 of the GDPR has established a parental consent requirement before the offering of 'information society services' directly to children under the age of 16 (unless a lower national age threshold between 13 and 16 applies).

Being new, the GDPR's parental consent requirement remains unclear and faces many practical implementation challenges. However, in the US since 1998 the Children's Online Privacy Protection Act (COPPA) has provided detailed rules for the operators of online services directed towards children that collect (or have actual knowledge that they collect) personal information from children. As the GDPR has been partially inspired by COPPA, US experience could inform the debate in the EU over the new data protection challenges related to children's consent in relation to online services. Thus, the aim of this article is to critically assess the provisions of the GDPR related to the consent of minors, and make a comparative analysis with the requirements stipulated in the US COPPA in order to identify

Bibi van den Berg and Bart Schermer (eds), *Minding Minors Wandering the Web: Regulating Online Child Safety*. Information technology and law series (24) (Springer with TMC Asser Press, 2014) 19.

[12]United Nations Convention on the Rights of the Child (adopted on 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3 (UN CRC).

[13]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) [2016] OJ L119/1.

[14]Data Protection revision process has started on 25 January, 2012, when the EC, amongst others, published a Proposal for a GDPR. On 21 October, 2013 the LIBE Committee of the European Parliament voted on the Draft Report prepared by the rapporteur Jan Philipp Albrecht. On 12 March, 2014 LIBE Report has been adopted by the European Parliament. On 15 June, 2015 the Council agreed on General Approach and on 9 November 9, 2015 on its negotiating position. On 15 December, 2015 the Parliament and the Council reached political agreement in trilogue. On 17 December 17, 2015 LIBE Committee voted on texts agreed during interinstitutional negotiations. On 8 April, 2016 the Council adopted its Position and Statement of the Council's reasons. On 12 April, 2016 LIBE Committee voted on Recommendation for 2nd reading and on 14 April, 2016 the Parliament adopted the GDPR in 2nd reading. On 27 April, 2016 GDPR was signed and on 4 May, 2016 published in the Official Journal of the European Union.

[15]For a more detailed description of the child specific protection regime in the GDPR see Milda Macenaite, 'From Universal Towards Child-Specific Protection of the Right to Privacy Online: Dilemmas in the EU General Data Protection Regulation' (2017) 19(5) New Media and Society 765.

pitfalls and lessons to be learnt before the new rules on the consent of minors in the EU become applicable.

This article is divided in five parts. The first part provides an overview of the context relating to the processing of children's personal data, especially in the online world. The second part explores the general notion of consent in the EU data protection law, including the conditions for a valid consent. In the third part, the legislative development of Article 8 of the GDPR dealing specifically with children's consent in relation to information society services is examined. The fourth part presents the US relevant legislative framework, that is, COPPA and its main requirements. In the fifth part, the challenges related to the practical implementation of the provision on the consent of minors in the GDPR will be discussed in light of the US experience. Finally, based on this comparison, we will conclude with some recommendations for the future application of the new rules on the consent of minors.

2. Conception of Article 8 – exploring the context

Since the adoption of Directive 95/46/EC in the pre-internet era which remained silent in relation to children, the regulatory context for the GDPR has drastically changed. In particular, there have been several driving factors (contextual and legal) behind the vast increase in attention for children's privacy protection on the Internet, that played a role in acknowledging children as special data subjects in the GDPR.

2.1. Contextual developments

Several developments can be seen as preparing the ground for the adoption of specific provisions in the GDPR relating to the protection of minors with regard to the processing of their personal data.

First, in recent years increased attention has been paid to children and their rights in EU policy making. The importance of promoting children rights has become a clear objective of the EU as stated in Article 3(3) of the TEU. In Article 24 of the European Charter of Fundamental Rights, the EU committed to safeguarding children's rights to protection and care. Moreover, the effective protection of children in all EU policies having an impact on their rights are identified among the main priorities in EU strategic documents.[16] These documents transform the EU policy objectives into actions. The need to ensure that children's rights are enhanced and respected in all the EU legislative proposals and decisions has been continuously acknowledged among the EU institutions. In fact, the EU Agenda for the Rights of the Child recognises as one of its objectives the achievement of 'a high level of protection of children in the digital space, including of their personal data, while fully upholding their right to access internet for the benefit of their social and cultural development'.[17] In 2015, the European Parliament and the Council called

[16]Commission (EC), 'European Strategy for a Better Internet for Children' (Communication) COM/2012/0196 final, 2 May 2012; Commission (EC), 'An EU Agenda for the Rights of the Child' (Communication) COM/2011/0060 final, 15 February 2011 (establishes the strong commitment of all EU institutions and of all EU Member States to promoting, protecting and fulfilling the rights of the child in all relevant EU policies, states that the standards and principles of the United Nations Convention on the rights of the child must continue to guide EU policies and actions that have an impact on the rights of the child, urges to take the 'child rights perspective' into account in all EU measures affecting children).

on the European Commission (EC) to present a new and comprehensive strategy and action plan on the rights of the child.[18] The commitment of the EU institutions to promoting, protecting and fulfilling children's rights in all relevant policy areas and actions means that the principles of the UN CRC should guide the EU policies directly or indirectly affecting children. In other words, children's rights considerations, such as the best interest of the child, should be taken into account in the drafting of legislative proposals.

Second, a significant increase in empirical data about children's internet use and related online risks has been gathered across Europe by the EU funded EU Kids Online project and became available for policy makers, academics and other stakeholders. In 2011, research indicated that 9% of children aged 11–16 experienced personal data misuse online and significant amount of children faced difficulties when finding and using reporting tools and privacy settings to protect themselves online.[19] In 2014, research reaffirmed that some of the most important concerns among children still remain related to personal data misuse and reputational damage, such as hacking of social media accounts, creation of fake profiles, and impersonation.[20]

Third, several inspections on the ground raised the concerns around a growing number of websites and mobile apps targeted at, or frequently used by, ever younger children and the lack of specific data protection rules that would take into account the unique needs of children as data subjects. In 2012, the Federal Trade Commission (FTC) in the US reviewed information provided to users by 400 kids' apps and revealed that many of them lacked transparency and clear disclosure about the children's data collection practices.[21] In 2015 during the time the GDPR was under debate in the Council, 29 data protection authorities (DPAs) from around the world carried out a Global Privacy Sweep (i.e. a joint review of 1494 websites and apps directed towards children).[22] The results revealed many problems, such as inadequate, non-child-tailored privacy policies, excessive collection of personal data from children, and the frequent disclosure of children's data to third parties. In relation to age verification and parental consent in services, the Sweep report stated that

> although many sites and apps claimed in their privacy policies to preclude access to children under a specified age, only 15% of websites and apps swept had age verification or gating to bar younger children from accessing the site or app. Sweepers also found that some of those controls did not function (e.g. a child indicating she was 10 years old could still access the site)

[17]Commission (EC), 'An EU Agenda for the Rights of the Child', COM/2011/0060 final, 15 February 2011, 10.

[18]European Parliament (EP), Resolution on the 25th anniversary of the UN Convention on the Rights of the Child, 2014/2919 (RSP), 27 November 2014 (called on the Commission to present 'an ambitious and comprehensive child rights strategy and action plan for the next five years'); Council of the European Union, Conclusions on the promotion and protection of the rights of the child, 15559/14, 4-5 December 2014 (called on the Commission to develop a renewed EU Agenda for the Rights of the Child in line with Better Regulation principles).

Anna Maria Corazza Bildt and others, Question for Written Answer to the Commission on Child Rights Strategy (2015–2020), E-005691-15, 9 April 2015 <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2015-005691+0+DOC+XML+V0//EN> accessed 9 April 2017.

[19]Sonia Livingstone and others, 'Risks and Safety on the Internet: The Perspective of European Children' (LSE, EU Kids Online, London 2011); Sonia Livingstone and others, 'Towards a Better Internet for Children: Findings and Recommendations from EU Kids Online to Inform the CEO Coalition' (LSE, EU Kids Online, London 2012).

[20]Mascheroni and Ólafsson (n 9).

[21]Federal Trade Commission (FTC), 'Mobile Apps for Kids: Current Privacy Disclosures are Disappointing' (Staff report), February 2012 <https://www.ftc.gov/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing> accessed 9 April 2017.

FTC, 'Mobile Apps for Kids: Disclosures Still Not Making the Grade', December 2012 <http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf> accessed 9 April 20.

[22]GPEN, '2015 GPEN Sweep – Children's Privacy', 2015 <http://194.242.234.211/documents/10160/0/GPEN+Privacy+Sweep+2015.pdf> accessed 9 April 2017.

> and others were only passive (e.g. a pop-up indicating that a child below a specified age should not access the site). Noteworthy, only 24% of sites and apps swept encouraged parental involvement.[23]

In response to these finding, some DPAs, such as the French DPA (CNIL), published guidelines[24] thereby sending a reminder to child-directed websites and services regarding their obligations in terms of *inter alia* parental consent for the collection of sensitive data and photographs from children and the transferring of data to third parties for marketing purposes. In the wake of the EU data protection reform, the results of the sweep could have helped to crystalise the final position on the protection of children's personal data online among the policy makers.

2.2. Lack of harmonisation within the EU

The Directive 95/46/EC failed to explicitly address the age limit of consent and as a result there has been lack of clarity on the matter in many EU countries. The question 'at what age can children consent to have their personal data processed' even became ironically called 'the million euro question' by European data protection experts.[25] Lack of harmonisation across the EU caused legal uncertainty among data controllers who were exposed to diverging legal rules when collecting children's personal data.[26] In the following paragraphs we will explore why setting the age of consent is a difficult issue and how this issue has been approached by national policy makers in the EU.

2.2.1. The concept of child and his legal capacity

Determination of the legal competence of minors to consent to data processing is a complicated task. The complexity of setting an age specific competence threshold stems from conceptions of childhood, including the ideas about children's needs and capacities and how they change with growth,[27] as well as national historical, cultural and social heritage of a particular country and legal system. In addition, as Hodgkin and Nowell have rightly noted

> setting an age for the acquisition of certain rights or for the loss of certain protections is a complex matter [which] balances the concept of the child as a subject of rights whose evolving capacities must be respected with the concept of the State's obligation to provide special protection.[28]

[23] ibid.

[24] Commission Nationale de l'Informatique et des Libertés (CNIL), 'Editeurs de sites pour enfants: n'oubliez pas vos obligations!', 2 September 2015 <https://www.cnil.fr/fr/editeurs-de-sites-pour-enfants-noubliez-pas-vos-obligations-0> accessed 9 April 2017.

[25] Giovanni Buttarelli, 'The Children Faced with the Information Society', 1st Euro Ibero American Seminar On Data Protection: "Children's Protection" Cartagena de Indias (2009) <https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2009/09-05-26_Cartagena_children_protection_EN.pdf> accessed 9 April 2017.

[26] European Data Protection Supervisor (EDPS), Opinion on the Communication 'A comprehensive approach on personal data protection in the European Union', 2011 <https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf> accessed 9 April 2017 (the EDPS claimed that the GDPR should include specific provisions on children to better protect their particular interests and provide legal certainty for data controllers).

[27] Arlene Skolnick, 'The Limits of Childhood: Conceptions of Child Development and Social Context' (1975) 39 Law and Contemporary Problems, 38.

[28] Rachel Hodgkin and Peter Newell, *Implementation Handbook for the Convention on the Rights of the Child* (UNICEF, 2002), 1.

Establishing a precise age limit after which the processing of personal data becomes subject to fewer or no additional legal constraints is not a challenge faced solely by data protection law. Other areas such as consumer contract law, family, civil, criminal, and administrative law, have also faced the question of whether, and if so, where a line indicating a particular age as the starting point of adulthood should be drawn. The UN CRC makes use of the term 'child', which it defines as 'every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier'. This position was also followed by the Article 29 Working Party, which considered a child as someone under the age of 18, unless they have acquired legal adulthood before that age. The EC's draft GDPR proposal incorporated the definition of the UN CRC, but this did not make it into the final version of the Regulation (discussed below). However, taking into account that the right to data protection belongs to the child and not to their representative (who is merely appointed to exercise them), legal incapacity until the age of 18 can be easily seen as overprotective. Following the requirements of the UN CRC, children should be increasingly consulted on matters relating to them and thus solutions for consent could range from mere consultation with the child, to parallel or joint consent of the child and a parent, or even to the autonomous consent of a mature child.[29] As a result, diverging age thresholds, rarely as high as 18, are explicitly introduced (or tacitly accepted in practice, depending on the Member State) for minors as data subjects while regulating their power to give a valid consent to the data processing operations. A large discrepancy exists with regard to the age, after which minors are legally competent to give their consent.[30] In general, many European countries consider minors ranging from 14 to 16 years to be competent to consent to the processing of their data. However, the precise question of whether a particular minor has given valid consent in a particular context might still depend on all the circumstances, including

> both subjective matters such as the maturity of the minor and more objective matters such as whether the matter for which consent was given was in the direct interest of the minor or not, and indeed whether the parents were, or should have been involved.[31]

2.2.2. Three distinct national choices

The lack of harmonised general rules on children's data processing and consent, opened the door for individual EU member states to nationally set their age limits at which parental consent is required and foresee how valid consent from minors should be obtained. Legal regulations or solely existing opinions and best practices on the age threshold for a valid consent of a minor notably differ across the EU Member States and the legal capacity to consent to data processing operations varies not only in different jurisdictions but also across sectors, like research[32] or advertising.[33]

[29]Article 29 Working Party (A29WP), 'Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools) WP 160', 11 February 2009.

[30]Terri Dowty and Douwe Korff, 'Protecting the Virtual Child – The Law and Children's Consent to Sharing Personal Data' (Study prepared for arCh – action on rights for Children- and the Nuffield Foundation), 2009 <http://www.nuffieldfoundation.org/sites/default/files/Protecting%20the%20virtual%20child.pdf> accessed 1 March 2017.

[31]ibid.

[32]As to the legal requirements and procedures for involving children in research, including in particular procedures of ethics approval and informed consent of children and their parents for all EU Member States see the Fundamental Rights Agency, 'Legal requirements and ethical codes of conduct of child participation in research in EU Members States', 2014 <http://fra.europa.eu/en/theme/rights-child/child-participation-in-research#80> accessed 10 April 2017.

The broad range of diverging practices among the EU Member States in the area of data protection may be divided into three groups in relation to the method and interpretation of the exact age threshold enabling minors to consent to their data protection.

2.2.2.1. An objective bright-line approach. A few Member States explicitly state in their national data protection law the exact age threshold from which minors are treated as legally competent to act as data subjects on their behalf. This regulatory choice can be called an objective bright-line rule.[34] In Spain, the data protection law contains specific provisions on the consent for the processing of data on minors.[35] According to Article 13 of the Spanish Personal Data Protection Law, 'data pertaining to data subjects over 14 years of age may be processed with their consent, except in cases when the law requires the assistance of parents or guardians'. The same article also forbids the collection of data from minors regarding members of their family or its members' characteristics, such as data relating to the professional activity of the parents, financial information, sociological or any other such data, without the consent of the persons to whom such data refers. The exception is data regarding the identity and address of the father, mother or guardian which may be collected for the sole purpose of obtaining their consent. The Spanish law also underlines the responsibility of the data controller for the setting up of the verification procedures that guarantee the age of the minor and the authenticity of the parental consent.

Similarly, although stipulated in less detail, the data protection law in the Netherlands states that

> (I)n the case that the data subjects are minors and have not yet reached the age of sixteen, or have been placed under legal restraint or the care of a mentor, instead of the consent of the data subjects, that of their legal representative is required. The data subjects or their legal representative may withdraw consent at any time. (Article 5 Dutch Data Protection Law)[36]

The Dutch DPA specified the obligation to obtain valid consent from those under the age of 16 online in its guidelines entitled 'Publication of personal data on the Internet' which was adopted in 2007.[37] The Dutch DPA does not specify or recommend concrete methods for obtaining the consent of a minor's parents or legal representatives, but underlines the general principle that the data controller must be able to demonstrate that consent has been obtained, alternatively consent is void and any subsequent processing of the personal data online is unlawful. It also points to a social responsibility of the website owners and network environments aimed at those under the age of 16 to explain the rights and obligations of their users in a clear and understandable language.

Additionally in Hungary, Section 6 sub-section 3 of the Hungarian Privacy Act[38] clearly states that '(T)he statement of consent of minors over the age of 16 shall be

[33]For example, UK's Advertising Standard Authority, The UK Code of Non-broadcast Advertising, Sales Promotion and Direct Marketing, Edition 12 <https://www.asa.org.uk/asset/47EB51E7%2D028D%2D4509%2DAB3C0F4822C9A3C4/> accessed 10 April 2017 (defines a child as an individual under 16).

[34]Lina Jasmontaite and Paul de Hert, 'The EU, children under 13 years, and parental consent: a human rights analysis of a new, age-based bright-line for the protection of children on the Internet' (2015) 5(1) International Data Privacy Law 20.

[35]Real Decreto 1720/2007 por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

[36]Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens).

[37]Dutch Data Protection Authority, 'Publication of Personal Data on the Internet' (guidelines), December 2007 <https://cbpweb.nl/sites/default/files/downloads/mijn_privacy/en_20071108_richtsnoeren_internet.pdf> accessed 8 May 2016 sub-section 4.1.

considered valid without the permission or subsequent approval of their legal representative'.

Finally, the UK Data Protection Act 1998, albeit not directly referring to the age of consent, has a special section on the exercise of rights in Scotland by children which states:

> where a question falls to be determined in Scotland as to the legal capacity of a person under the age of sixteen years to exercise any right conferred by any provision of this Act, that person shall be taken to have that capacity where he has a general understanding of what it means to exercise that right.

It further specifies: 'a person of twelve years of age or more shall be presumed to be of sufficient age and maturity to have such understanding'.[39]

All four of the above-mentioned EU countries introduced the age limit for consent of minors as a general requirements, without making a specific reference to consent in the online environment. Thus, this requirement is equally applicable to data processing online.

2.2.2.2. 'Regulation by analogy' approach. Some other Member States chose the 'regulation by analogy' model and invoke civil law provisions establishing when a person becomes fully competent to acquire and assume rights and obligations and apply them to the area of data protection. For example, in Lithuania children can be considered as competent from 14 years old, as from that age they enjoy partial rights and are allowed to carry out basic legal acts without the consent of their representatives. Consequently they are also allowed to consent to some basic personal data processing operations.[40]

2.2.2.3. Subjective capacity-based approach. Many Member States seem to have no bright-line specific provision or rely on the legal capacity of agents in other branches of law but instead assess the concrete situation on case-by-case basis applying the general criteria of the best interest of the child, level of moral and psychological development, the capacity to understand the consequences of giving consent and evaluating specific circumstances (the age of the child, the purpose of data processing, type of personal data involved,[41] etc.). Such an evaluation of the capacity of the data subject is a subjective and context-specific test rather than one that is universally applicable, but assumption-based exemplar age thresholds are normally set in case law, legal doctrine or guidelines from the DPAs. This choice can be called the subjective capacity test. For example, in the UK, there is a general presumption that no assumptions about an individual under 16 can be made as they lack legal capacity. Although there is no case law about children's capacity to consent to data processing, the existing case law developed some guidance on the situations

[38]Hungarian Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information.

[39]Section 66 of the Data Protection Act 1998. For the explanation of this, rather confusing, section see Dowty and Korff (n 30) 15–16.

[40]M Macenaite and others, *Vaiku privatumo apsauga internete* (Lithuanian Consumer Institute, Vilnius 2011) 33, 69.

[41]In Austria, for example, there are no legal restrictions or case law, although the age of 14 is usually taken as the cut-off point below which consent is required, except for the processing of sensitive data, for which parental consent is required for all minors.

in which children can give consent to a medical treatment or legal representation.[42] The seminal case on the matter is *Gillick v. West Norfolk and Wisbech Area Health Authority*. This case developed guidelines under which a doctor can lawfully provide contraception to a girl under 16 years old without informing her parents. It established a principle that children under 16 can sometimes give their consent to certain things, but there is no fixed age when one can presume the competence of a child.[43] In the UK, the Data Protection Act 1998 does not deal with the issue of obtaining consent from children. The main document providing guidance with regard to data collection online is issued by the UK Information Commissioner's Office (UK ICO) through the Personal Information online code of practice adopted in 2010. The code states that 'assessing understanding, rather than merely determining age, is the key to ensuring that personal data about children is collected and used fairly'. When services are directed at children, the UK ICO advises: to determine the level of understanding of the child rather than only the age; to require parental consent for children under the age of 12; to collect information in a way that children understand and to which parents are not likely to object. When the information obtained from the child is relatively speaking of less importance or sensitivity (such as name), then simple notification of parents via email is enough, whereas when a photograph of the child is being processed then something more akin to verifiable parental consent is necessary. In Belgium the issue of minors' consent has been addressed in an Advice issued by the Belgian DPA.[44] The Advice states that even though under Belgian law, the age of maturity is 18 years, the gradual development of minors and the need for more independence with growth should be acknowledged, especially in adolescence, between the ages of 13 and 16 years. When a child is not mature enough to be able to understand the implications of the given consent parental consent is necessary. For those younger than 13 or 14 consent is required in all cases, however in complicated cases parental consent is also mandatory for children younger than 15 years. Parental consent should also be gained when sensitive data are collected from those under 16, and in all cases when data processing is not in the interest of the child.

At a European level, the approach is similar to the majority of the national jurisdictions described in the third group. The Article 29 Working Party in the Opinion dedicated to the protection of children's privacy,[45] took a similarly flexible approach and did not set precise age limits at which parental consent is required. Instead, it underlined the importance of the maturity of a child and complexity of the data processing at hand. For instance, the Article 29 Working Party believed that data collection from an 8-year-old child for the purpose of sending a free magazine or newsletter does not require parental consent, while such consent would be necessary for the same child to take part in a live TV show.

[42]Dowty and Korff (n 30) 8.

[43]LSE Working Group on Consumer Consent, 'From Legitimacy to Informed Consent: Mapping Best Practices and Identifying Risks' (2009) <http://www.lse.ac.uk/management/documents/research/research-initiatives/Report-on-Online-Consent.pdf> accessed 3 March 2017, 54–55.

[44]Belgian Privacy Commission, 'Advice No. 38/2002 of 16 September 2002 Concerning the Protection of the Private Life of Minors on the Internet' (2002) <http://www.privacycommission.be/nl/docs/Commission/2002/advies_38_2002.pdf> (Dutch); <http://www.privacycommission.be/fr/docs/Commission/2002/avis_38_2002.pdf> (French), accessed 1 March 2017.

[45]Article 29 Data Protection Working Party, 'Opinion 2/2009 on the Protection of Children''s Personal Data (General Guidelines and the Special Case of Schools) WP 160', 11 February 2009.

3. Consent in EU data protection law

3.1. The concept of consent

The consent of the data subject as a legitimate basis for personal data processing is recognised in the Charter of Fundamental Rights (CFR) of the EU[46] and further in the Data Protection Directive (Article 7 DPD). The GDPR retains consent of the data subject as one of the grounds for lawful processing of personal data (Article 6(1)(a) GDPR).

The consent of the data subject in the context of the Data Protection Directive is understood as 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed' (Article 2 (h) DPD). The definition of consent in the GDPR remains very close to the definition of the term in the DPD:

> 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. (Article 4 (11) GDPR)

The Article 29 Working Party closely examined the concept of consent in the DPD in its opinion on the definition of consent,[47] specifying and examining the criteria for the consent of the data subject to be valid. According to the Article 29 Working Party, the consent must be (a) an indication of the wishes of the data subject … signifying … , (b) freely given, (c) specific, and (d) informed. These elements will now be briefly discussed as they remain identical to the definition of consent contained in the GDPR and will be then followed by a short discussion of the 'unambiguous' qualification.

(a) Indication of the wishes of the data subject

An essential element in deciding if the data subject consents to a specific processing operation is the examination of whether there is a clear indication of the wishes of the data subject. The GDPR clarifies in the definition of consent that data subject should indicate his wishes using a statement or a clear affirmative action (Article 4(11) GDPR). Therefore consent cannot be inferred from the absolute silence of the data subject. Similarly pre-ticked boxes or lack of any action on behalf of the data subject does not constitute consent (Recital 32 GDPR). Recital 32 GDPR clarifies that an indication of the wishes of the data subject can be provided

> by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. […] If the data subject's consent is to be given following a request by electronic means, the request

[46]The CFR of the EU, which came into force on 1 December 2009, besides a right to private life (Article 7), recognised the protection of personal data as a separate right under its Article 8. Article 8 of the Charter safeguards the protection of personal data and Article 8 Part 2 stresses the processing of personal data on the basis of consent or other legitimate grounds by stating:

> 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.

[47]Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent, WP 187', 13 July 2011.

> must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided. (Recital 32 GDPR)

(b) Freely given consent

There are various influences that can be exercised on data subjects in order to manipulate their decision to agree to the processing of their personal data. However, not every exercise of external pressure leads to invalidation of consent. The consent of the data subject is still freely given when positive pressure is exercised, while the exercise of any kind of negative pressure renders the consent invalid. Recital 42 GDPR clearly summarises that '[c]onsent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment'. The GDPR clearly stipulates that in order to assess whether consent in freely given

> utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of the contract. (Article 7(4) GDPR)

Similarly consent will not be deemed to be freely given if this relates to more than one data processing operation and it is not possible to separate out consent on the basis of each individual data processing operation (Recital 43). Moreover recital 43 clarifies that consent should not be considered as freely given and the processing of personal data should not rely on it when there is clear imbalance between the data subject and the data controller 'in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation'. (Recital 43 GDPR)

(c) Informed consent

The provision of adequate information to the data subject is context-related. The types and amount of information should be decided on a case-by-case basis in the light of the fairness principle. That being said, the information that is specified in Article 13 GDPR should be provided to data subjects irrespective of the circumstances as complemented by any other information that is required in order to properly informed the data subjects vis-à-vis the specific circumstances of the processing. The information should be easily accessible, easy to understand and should be provided in an intelligible form (Recital 39 GDPR). Recital 39 GDPR provides a short description of the transparency principle and indicates that this in particular concerns the provision of

> information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. (Recital 39 GDPR)

In the context of the novelties introduced in the GDPR where risk plays a prominent role in the handling of personal data, the GDPR requires that specific information is provided to the data subjects with regard to the risks, conditions of processing, relevant safeguards in place as well as the rights of the data subjects in relation to the processing of personal data (Recital 39 GDPR). In particular the provision of information to children, in light of the fairness principle, should be adapted to children, in order to make it easy for them to

understand what information is collected about them and for what purposes it will be used.[48]

(d) Specificity of consent

The GDPR provides that the consent of the data subject should be specific. The requirement for specificity relates to all circumstances surrounding the processing of the personal data for which the consent is been sought. The specification of the information that is provided to the data subject is an intrinsic element of the requirement for informed consent. However, the element that the consent has to be specific also relates to the degree of specificity it has to ascertain. Valid consent requires the explicit specification of the aimed legitimate purposes (recital 39 GDPR). It is unclear to what extent clearly specified consent, covering for instance multiple purposes, could be invalid. On this point the GDPR clarified that multiple processing operations that are carried out for the same purpose(s) can be covered under one consent (Recital 32 GDPR). Similarly, when a processing operation is carried out for multiple purposes, then consent should be provided for all of them (Recital 32 GDPR).

The definition of consent in the GDPR includes the additional requirement that consent needs to be unambiguous, a qualification that was required only in two instances under the Data Protection Directive: when consent was the ground for legitimate processing of personal data (Article 7(a) DPD) and in the context of transfers of data to third countries (Article 26(1) DPD). Several Member States, such as Germany and the United Kingdom, chose not to incorporate the qualification of 'unambiguously given' consent in their national data protection legislation when transposing the Data Protection Directive. Kosta claims that

> The additional condition that the consent should be given 'unambiguously' does not add any real value to the way how consent should be interpreted. A consent given 'ambiguously' would amount to an unclear indication of the wishes of the data subject for processing of his personal data and would not qualify as valid consent.[49]

The EC in its Proposal for the GDPR introduced the element that consent has to be 'explicit' in the definition of the term,[50] a proposal that was also welcomed by the European Parliament in its first reading.[51] The Council of the EU in its first reading did not include either the qualification of unambiguous or explicit consent. However, as already discussed, the final version of the GDPR, which resulted from the Trialogue debates, included a qualification of unambiguous consent in the definition of the term, despite the controversy as to whether this qualification has any actual value.

[48]Article 29 Working Party, 'Opinion 15/2011 on the Definition of Consent WP 187', 13 July, 2011, 37; Recital 58 of the GDPR: 'Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand'.

[49]Eleni Kosta, *Consent in European Data Protection Law* (Brill/Martinus Nijhoff Publishers, 2013), 235.

[50]Commission (EC), Proposal for a Regulation of the European Parliament and of the 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 (Draft Data Protection Regulation), 25 January 2012.

[51]European Parliament (EP), Legislative resolution on the proposal for a regulation of the European Parliament and of the 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)0011 – C7-0025/2012 – 2012/0011(COD)) (Ordinary legislative procedure: first reading), 12 March 2014.

3.2. Special conditions for consent

In Article 7 the GDPR sets out specific conditions with regard to the provision of consent that are also of high relevance in the context of the consent of minors. The GDPR clarifies that the data controller must be able to demonstrate that the consent of the data subject has been provided for specified purposes (Article 7(1) GDPR). As the data controllers will be responsible to prove that the consent of the data subject was provided in a valid way for a specific data processing operation, they should also use reliable means in order to obtain the consent, taking into account the sensitivity of each specific data processing operation.[52]

The GDPR also introduces the rule that when data subject consent is provided as part of a written declaration that concerns another matter, then the request for consent has to be presented in a clearly distinguishable form from the other elements of that written declaration in an intelligible and easily accessible form, using clear and plain language (Article 7(2) GDPR). This new rule is already to be found in Germany, where the German Federal Court of Justice published a decision on the 'Payback' case, according to which it was sufficient that the clause on the consent to the processing of personal data was clearly highlighted and the data subject was given the opportunity to object to such processing.[53] The clause on consent to data processing should not be simply part of the general terms and conditions of a contract, without any special highlighting,[54] nor can it be included in the fine print of the contract, as the data subject can easily overlook it.[55] According to Article 7(3) GDPR the data subject has the right to withdraw his consent at any time; however the withdrawal does not affect the lawfulness of the processing that was based on consent before the withdrawal (Article 7(3) GDPR).

The application of the general requirements for a valid consent (as mentioned above) is complex. However, this complexity is further intensified in the context of the consent of minors in the online environment. For example, the requirement of a freely given consent becomes more complicated in circumstances where children could give their consent without the involvement or knowledge of parents and this is particularly problematic given that very often their choices may be manipulated and vulnerabilities exploited for commercial purposes due to their increasing spending power.[56] Fulfilling the requirements for informed consent is particularly challenging in case of minors, as their level of understanding and ability to foresee possible consequences differs from adults. Although the use of privacy policies is a common practice and many of them formally follow legal requirements regarding the obligatory information, it is doubtful whether they achieve

[52]European Data Protection Supervisor, 'Opinion on the Data Protection Reform Package', 7 March 2012, para 129.

[53]Bundesgerichtshof (GERMBGH – German Federal court of Justice), Decision of 16 July 2008, Az: VIII ZR 348/06 ('Payback'), MMR 2008, 731.

[54]Helmut Redeker, 'Teil 12 Internetverträge' in Thomas Hoeren and Ulrich Sieber (eds), *Handbuch Multimedia-Recht – Rechtsfra-gen des elektronischen Geschäftsverkehrs* (Ergänzungslieferung) (2010), para 111.

[55]Bundesgerichtshof (BGH – German Federal Court of Justice), Decision of 16 July 2008, AZ: VIII ZR 348/06 ('Pay-back'), MMR 2008, 733; Peter Gola and Rudolf Schomerus BDSG – Bundesdatenschutzgesetz, Kommentar (8th edn 2005) Section 4a, para 14; Spiros Simitis (ed), Kommentar zum Bundesdatenschutzgesetz (5th edn 2003), Section 4a, para 40; Thomas Hoeren, 'Die Einwilligung in Direktmarketing unter datenschutzrechtlichen Aspekten' (2010) Zeitschrift für die An-waltspraxis, 434.

[56]Kathryn C Montgomery, 'Youth and Surveillance in the Facebook Era' (2015) 39(9) Telecommunications Policy 771; Valerie Steeves and Ian Kerr, 'Virtual Playgrounds and Buddybots: A Data-Minefield for Tinys & Tweeneys', Panopticon, 15th Annual Conference on Computers, Freedom & Privacy, Keeping an Eye on the Panopticon: Workshop on Vanishing Anonymity, Seattle, 12 April 2005.

their goal.[57] However, even with extensive information available and especially given the complexity of profiling techniques and big data analytics that are difficult even for adults to comprehend, many minors would still be unable to properly measure the significance of their consent as regards the impact on their privacy and personal autonomy. Many privacy policies are long, hard to find and navigate, written in complicated language and are beyond the capacity of an average adult to understand.[58]

4. Legislative history of article 8

The GDPR devotes a specific Article to the processing of the personal data of children which pays special attention to issues related to consent. The legislative history of Article 8 of the GDPR is thin. It seems that the majority of the debates during the GDPR legislative process focused more around articles with a direct economic impact on data controllers' activities and the Digital Single Market, such as the one-stop-shop mechanism or profiling, rather than protection of vulnerable data subjects. Article 8 witnessed sporadic renewals of interest during the debates and clearly lacked well-reasoned justifications and evidence before adoption. Nevertheless, this section aims to chronologically delve into the positions of the EU institutions involved in the legislative process and the changes they proposed to Article 8.

4.1. Commission proposal

A first unofficial version of the EC Proposal for the GDPR[59] was leaked online in December 2011 by StateWatch. In this text a child was defined as any person under 18 years (Article 3 Part 18). This definition echoed the understanding of childhood in accordance with the UN CRC. That version of the GDPR did not contain any specific articles on the processing of the personal data of a child. Instead, Paragraph 6 of Article 7 which specified the conditions for consent established that the consent of a child is only valid when given or authorised by the child's parent or custodian. This approach demonstrates that at the beginning of the data protection reform process the EC had no intention of differentiating between digital and offline consent and aimed at protecting equally everyone below the age of 18. The same is confirmed in the questions that the EC posed to the key stakeholders in the targeted consultation meetings in 2010, asking if 'a harmonized age limit of 18 years in line with Article 1 of the UN Convention on the Rights of the Child' should be adopted to better protect the personal data of minors.[60]

[57]Patrick Van Eecke and Maarten Truyens, 'Privacy and Social Networks' (2010) 26 Computer Law & Security Review, 542.

[58]UK Children's Commissioner, 'Growing Up Digital: A Report of the Growing Up Digital Taskforce' (January 2017) <http://www.childrenscommissioner.gov.uk/sites/default/files/publications/Growing%20Up%20Digital%20Taskforce%20Report%20January%202017_0.pdf> accessed 9 April 2017; Jacquelyn Burkell, Valerie Steeves and Anca Micheti, 'Broken Doors: Strategies for Drafting Privacy Policies Kids Can Understand' (report), March 2007 <http://www.idtrail.org/content/view/684/42/> acessed 10 April 2017, 1–2.

On privacy policies in social networks in general see, Joseph Bonneau and Sören Preibusch, 'The Privacy Jungle: On the Market for Data Protection in Social Networks' (The Eighth Workshop on the Economics of Information Security, London, 24 June 2009) <http://www.jbonneau.com/doc/BP09-WEIS-privacy_jungle.pdf> accessed 9 March 2017.

[59]Proposal for a Regulation of the European Parliament and of the 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) Version 56 (29/11/2011) <http://statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf> accessed 10 April 2017.

[60]Commission (EC), 'Stakeholders' Consultations "Future of Data Protection"' (background paper) <http://ec.europa.eu/justice/news/events/data_protection_regulatory_framework/background_paper_en.pdf> accessed 10 April 2017, question 4.

The Proposal for a GDPR,[61] officially presented by the EC on 25 January 2012, retained the definition of a child as any person below the age of 18 years (EC proposal GDPR). However, just before publishing the Proposal (during the Commission inter-service consultation process) an amendment to the article on consent was unexpectedly introduced and a new Article on the processing of the personal data of a child was added to the GDPR.

In relation to the offering of information society services directly to children, the age limit at which the personal data of a child cannot be processed without parental consent was lowered to 13 years (Article 8 Part 1). The European Data Protection Supervisor (EDPS) found this approach 'reasonable',[62] while the Article 29 Working Party suggested that the scope of application of this provision was broadened in order to cover other areas where the processing of personal data of children is taking place, outside the provision of information society services.[63] According to the EC proposal the EC would have retained the power to specify concrete methods to obtain valid consent for the processing of the personal data of children[64] and to publish delegated acts specifying the criteria and the conditions under which the consent of a child can be provided in a valid way.[65] The EDPS, however, expressed concerns with such delegated acts that would specify criteria and requirements for the methods in order to obtain verifiable consent in relation to the specific measures which the Commission might envisage for micro, small and medium-size enterprises.[66]

4.2. European parliament first reading

The Commission's draft GDPR proposal was subject to intensive discussions and lobbying at the European Parliament. In the Civil Liberties, Justice, and Home Affairs (LIBE) Committee alone 3999 amendments to the GDPR were proposed. On the 21st of October 2013, the LIBE Committee adopted the amendments to the EC proposed Regulation, including amendments to Article 8. The amendments proposed by the LIBE Committee were almost unanimously approved in the first reading of the European Parliament on 12 March 2014.[67]

Despite the amount of amendments registered, the discussions at the European Parliament (EP) did not lead to major substantive changes for Article 8 but instead only to small modifications. The EP, in essence, avoided questioning the necessity of having parental control through consent or indeed adopting a more nuanced version. It also refrained from publicly debating the reason of limiting the parental consent requirement to children below the age of 13 or questioning the burden and ineffectiveness of the parental consent mechanisms. The EP mainly introduced a specific information obligation requiring that information be 'provided in a clear language appropriate to the intended audience' (Article 8(1a) EP first reading). It also deleted the authority of the EC to adopt

[61]Commission (EC), Draft Data Protection Regulation, COM (2012) 11 final.
[62]European Data Protection Supervisor (n 52) para 128.
[63]Article 29 Data Protection Working Party, 'Opinion 01/2012 on the data protection reform proposals WP191', 23 March 2012, 13.
[64]Article 8(4) and Recital 130 draft Data Protection Regulation.
[65]Article 8(3) and Recital 129 draft Data Protection Regulation.
[66]European Data Protection Supervisor (n 52) para 81.
[67]European Parliament, Legislative resolution on the proposal for a regulation of the European Parliament and of the 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)0011 – C7-0025/2012), 12 March 2014.

implementing acts with standard forms for verifiable consent. Instead it designated the European Data Protection Board (EDPB) as responsible to issue guidelines, recommendations and best practices on how verifiable consent can be obtain or for verifying consent (Article 8(3)3).

However, there were amendments that were tabled in relation to these issues but these were not included into the final text. A group of Parliament members (MEPs) proposed to specifically underline that the protection of children is particularly important in social networks.[68] Other such amendments highlighted that

> the industry should take its shared responsibility to come up with innovative solutions, products and services in order to increase the safeguards on protection of personal data, in particular for children, for example through codes of conducts and monitoring mechanisms.[69]

One group of the MEPs proposed to delete Article 8 from the text of the GDPR.[70] The age of a child was questioned by five MEPs who proposed to raise the age limit for parental consent from 14 to 15 or 16 years.[71] One MEP suggested to increase the age limit up to 18, but to limit the scope of application (exempt services that 'are particularly appropriate and suitable for a child and have been notified and are controlled by the relevant national authorities' from consent requirement) and to accept unreliable consent methods (parents' consent via email).[72]

Notwithstanding the amendments proposed by a number of MEPs, the EP in its first reading made only the following changes. First, it expanded the scope of application of Article 8 and imposed the obligation to obtain parental consent to data controllers processing children's data in the offline world, when offering 'goods or services' directly to children rather than 'information society services'. In such a way, the EP followed the suggestion of the Article 29 Working Party to cover other areas where the processing of the personal data of children is taking place, outside the provision of information society services.[73] Second, the EP required data controllers to give information to children, parents and legal guardians in a clear, audience-appropriate language. As a result, the European Parliament amendments strengthened consent as an informed indication of wishes, in particular in respect to children.[74] A similar provision already existed in the EC proposal (Article 11) but was formulated in general terms and applicable to all data subjects. Third, the EP modified Recital 38 (previously Recital 29) by deleting a reference to the UN Convention on the Rights of the Child as a document from which the definition to determine when an individual is a child should be taken. This deletion did not substantially

[68] Committee on Civil Liberties, Justice and Home Affairs (LIBE), Amendments (1) 351 – 601, 2012/0011(COD), 4 March 2013 <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%2BCOMPARL%2BPE-504.340%2B01%2BDOC%2BPDF%2BV0%2F%2FEN> accessed 1 March 2017, Amendment 426 by Marian Harkin and Seán Kelly, and Amendment 427 by Sabine Verheyen and others.

[69] ibid, Amendment 521 by Anna Maria Corazza Bildt and Carlos Coelho.

[70] LIBE, Amendments (3) 886-1188, 2012/0011(COD), 4 March 2013 <http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/am/928/928600/928600en.pdf> accessed 10 April 2017, Amendment 1005 by Timothy Kirkhope on behalf of the ECR Group.

[71] ibid, Amendment 1006 by Csaba Sógo (the age of 14 years), Amendment 1008 by Manfred Weber (the age of 15 years), Amendment 1009 by Birgit Sippel, Petra Kammerevert and Josef Weidenholz (the age of 16 years), Amendment 1012 by Jean Pierre Audy, Seán Kelly (the age of 15 years).

[72] ibid, Amendments 1014 and 1019 by Axel Voss.

[73] Article 29 Data Protection Working Party, 'Opinion 01/2012 on the data protection reform proposals (WP191)', 13.

[74] LIBE, Compromise Amendments to the GDPR, A7-0402/2013, 21 October 2013, Article 8 para 1a.

change anything, as the definition of a child as an individual under 18 years of age still remained in Article 4(18).

The EP also added an emphasis on grounds other than consent for the lawful processing of the personal data of children: 'other grounds of lawful processing such as grounds of public interest should remain applicable, such as for processing in the context of preventive or counselling services offered directly to a child'.[75] This shows that the MEPs realised that certain services are created for children who seek help and must be used without their parents' consent, especially in situations where their parents might be closely linked to the problem, such as online-chats for victims of sexual abuse.[76] In other cases, when the interest of parents and children may not coincide consent may also not be the best ground for lawful data processing. This provision partly follows the suggestion of the EP Legal services and Internal Market and Consumer Protection committees which proposed exceptions to the parental consent rule in case of health data processing and social care.[77] The justification was that

> in the context of health and social care authorisation from a child's parent or guardian should not be necessary where the child has the competence to make a decision for him or herself. In Child Protection Cases it is not always in the interests of the data subject for their parent or guardian to have access to their data, and this needs to be reflected in the legislation.[78]

A similar amendment was tabled by two MEPs who proposed to adopt an exemption for parental consent in the context of health and social care where the child has the maturity and competence to make a decision on their own.[79] It was stressed, that in the UK, for example, a person of 12 years is presumed to be old and mature enough to exercise the right to decide who else can access their health records.

Noteworthy here is a sliding scale approach to consent proposed by the Legal service of the EP. The proposal took a risk-based approach and recognised various possible forms of consent instead of subjecting consent to a single rule. It stated that 'the appropriate form for obtaining consent should be based on any risk posed to the child by the amount of data, its type and the nature of the processing'.[80] This proposal was in line with the approach of the Article 29 Working Party.[81] The Article 29 Working Party proposed that the mechanism that would be used for age verification in the online environment each time should depend on various factors relating to the specific data processing operation, such as the types of personal data that will be processed, the purposes for which they will be processed, eventual risks arising from the processing etc.[82]

[75]EP Resolution (n 67), Recital 29.
[76]LIBE Amendments (3) 886-1188 (n 70), Amendment 1021 by Birgit Sippel, Petra Kammerevert and Josef Weidenholze.
[77]EP, Opinion of the Committee on Legal Affairs, Amendment 56, 25 March 2013, Opinion of the Committee on the Internal Market and Consumer Protection, Amendment 89, 28 January 2013 <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2013-0402&language=EN#title6> accessed 10 April 2017 (states that the authorisation from a child's parent or guardian should not be necessary 'where the processing of personal data of a child concerns health data and where the Member State law in the field of health and social care prioritises the competence of an individual over physical age').
[78]ibid.
[79]LIBE Amendments (3) 886-1188 (note 70), Amendment 1030 by Claude Moraes and Glenis Willmot.
[80]EP, Opinion of the Committee on Legal Affairs, Amendment 55, 25 March 2013 <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2013-0402&language=EN#title6> accessed 10 April 2017.
[81]Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent, WP 187', 13 July 2011, 28.
[82]ibid.

4.3. Council of the EU drafts

The most heated debates on the future of Article 8 of the GDPR took place in the Council of the EU. While the European Parliament proposed only revisions to the existing text of the EC focusing on the scope of its application, in the Council of the EU substantial debates among the Member States arose around the actual necessity to include any provisions on minors' consent in the GDPR.[83] The drafts of the GDPR published by two different presidencies contain evidence of debates that took place among Member States around Article 8 of the GDPR. A revised version of the draft GDPR published by the Greek Presidency on 30 June 2014, reveals that Member States had opposing opinions on the issue.[84] Seven Member States (Czech Republic, Germany, Austria, Sweden, Slovenia, Portugal, and the UK) held a scrutiny reservation and two countries (Czech Republic and Slovenia) wished Article 8 deleted. Norway[85] proposed in line with its national data protection law[86] the inclusion of a general provision prohibiting the processing of the personal data relating to children in a manner that is contrary to the child's best interest, instead of a specific article on children's consent. Such a provision, it claimed, would allow broader protection as the supervisory authorities would be able to intervene also in cases where, for example, 'adults publish personal data about children on the Internet in a manner which may prove to be problematic for the child'. Three Member States (Germany, Slovenia and Romania) suggested raising the age limit for consent from 13 to 14 years.[87]

The draft published by the Latvian Presidency of the Council[88] on 11 June 2015 was the basis for the General Approach of the Council on the GDPR. It demonstrated the crystallisation of three diverging views among Member States in relation to article 8. Now more Member States voiced a preference to have Article 8 deleted (Czech Republic, Malta, Spain, Slovenia and UK). Potential reasons of their preference to abandon the article relate to the difficulties to unanimously define a child in different EU countries and practical challenges relating to age verification and content obtaining mechanisms.

A larger group of Member States took a middle ground position as they expressed understanding of the merit and would have liked to see a provision on child protection in some form (Austria, Belgium, Cyprus, Germany, Greece, Hungary, Ireland, Italy and

[83]Council of the European Union, Note from Presidency to JHA Counsellors meeting (DAPIX) – Chapter II, 17072/3/14 REV 3, 26 February 2015 <http://data.consilium.europa.eu/doc/document/ST-17072-2014-REV-3/en/pdf> accessed 10 April 2017.

[84]Council of the European Union, Note from Presidency to Working Party on Information Exchange and Data Protection, 11028/14, 30 June 2014 <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011028%202014%20INIT> accessed 10 April 2017.

[85]Norway, although not being an EU country, participated in the debate on the GDPR as it will be applicable to Norway as part of the European Economic Area (EEA) together with Iceland and Liechtenstein.

[86]Norway on 20 April 2012 (Act of 20 April 2012 no. 18., effective 20 April 2012 under Royal Decree 20 April 2012 no. 335) amended its Personal Data Protection Act and among other changes included a provision which strengthens the protection of children's privacy beyond specific reference to their consent. Under the section 11, one of the basic requirements to process personal data, such as explicit purpose, data adequacy, relevancy is the requirement tailored to children as data subjects (i.e. 'Personal data relating to children shall not be processed in a manner that is indefensible in respect of the best interests of the child'.).

[87]Several delegations (Germany, France, Hungary, Luxembourg, Latvia, Romania, Slovenia) questioned the age of consent being set at 13 years. EC clarified that the choice was based 'on an assessment of existing standards, in particular in the US relevant legislation (COPPA)'. Council of the European Union, Note from Presidency to Working Party on Information Exchange and Data Protection, 11028/14, 30 June 2014, 87–88.

[88]Council of the European Union, Note from Presidency to the Council, Proposal for a Regulation of the European Parliament and of the 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) – Preparation of a general approach 9565/15, 11 June 2015 <http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf> accessed 10 April 2017.

Romania).[89] The third group of states took a different turn and instead of strengthening and clarifying parental consent, it proposed adding a limitation on certain data gathering and processing practices in relation to minors (profiling and marketing). France, supported by Estonia, Denmark, Sweden and Poland, suggested deleting Article 8 and instead inserting a particular provision for children when the Articles of the data subjects' rights were discussed, for example in Article 20 on profiling.

The Council draft from the 11th of June 2015 recognised the need for the special protection of children especially in relation to 'the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of child data when using services offered directly to a child' (Recital 29).[90] However, the definition of a child as any person below the age of 18 years was deleted from the list of definitions. The Council changed back the scope of Article 8 to focus on children's consent in relation to information society services. In such cases consent must be 'given or authorised by the holder of parental responsibility over the child or is given by the child in circumstances where it is treated as valid by Union or Member State law' (Article 8(1)). In this way the Council left it up the Member States to specify the age and the conditions for considering the consent for the processing of personal data of children valid. Moreover, it made it a responsibility of the data controller to verify that consent is provided or authorised by the person that holds parental responsibility over the child (Article 8(1a)). The Council did not include any provision detailing a Commission or EDPB responsibility to issue guidelines or best practices regarding the obtaining of verifiable consent or on the verification of such consent.

Initially, the Council kept the age limit for parental consent of 13 years that was first introduced by the EC, but a last-minute change raised the age of consent to 16 years.[91] This change generated public outrage, especially among children's rights activists, companies and youths themselves on social media. The provision was interpreted as banning kids from social media and even as being an attack on their human rights (i.e. such as freedom of expression and right to information).[92] In view of the meeting of the Committee of Permanent Representatives on 9 December 2015, the final GDPR draft opted for a compromise: the age of consent was set at 16 years, but allowed Member States to set a lower age which could not go below 13 years.[93] Thus, unless otherwise provided by

[89]ibid.

[90]ibid.

[91]Council of the European Union, Note from Presidency to Permanent Representative Committee, Proposal for a Regulation of the European Parliament and of the 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) [first reading] – Preparation for trilogue, 14902/15, 4 December 2015 <http://data.consilium.europa.eu/doc/document/ST-14902-2015-INIT/en/pdf> accessed 10 April 2017.

[92]danah boyd, 'What If Social Networking Becomes 16+?: New Battles Concerning Age of Consent Emerge in Europe', 18 December 2015 <https://medium.com/bright/what-if-social-media-becomes-16-plus-866557878f7#.si0ns0e2x> accessed 1 April 2017; Sonia Livingstone, 'No More Social Networking for Young Teens?', 18 December 2015 <http://blogs.lse.ac.uk/mediapolicyproject/2015/12/18/no-more-social-networking-for-young-teens/> accessed 10 April 2017; Janice Richardson, 'European General Data Protection Regulation Draft: The Debate', 10 December 2015 <https://medium.com/@janicerichardson/european-general-data-protection-regulation-draft-the-debate-8360e9ef5c1#.1jespbnno> accessed 10 April 2017; Larry Magid, 'Europe's New Privacy Regulations May Limit Teens', 17 December 2015 <http://www.connectsafely.org/europes-new-privacy-regulations-may-limit-teens/> accessed 10 April 2017; Samuel Gibbs, 'Is Europe Really Going to Ban Teenagers from Facebook and the Internet?', *The Guardian*, 15 December 2015 <https://www.theguardian.com/technology/2015/dec/15/europe-ban-teenagers-facebook-internet-data-protection-under-16> accessed 10 April 2017.

[93]Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data

Member State law, controllers must obtain the consent of a parent or guardian when processing the personal data of a child under the age of 16. The only reference to the change in the Council documents that can be found states: '[…] on the conditions applicable to consent given by a child, the co-legislators converged on keeping "below the age of 16 years" as a common ceiling, while allowing Member States to foresee lower age limits'.[94]

On the 15th of June 2015 the Council agreed on a General Approach on the GDPR based on the draft of the 11th of June 2015 and the Presidency of the Council received in this way a negotiating mandate to enter into the trialogue phase with the European Parliament and Commission. The trialogue resulted in a compromise text that was presented on 15th of December 2015.[95] The focus of Article 8 remained on information society services. Aside from the statement that children deserve specific protection of their personal data due to their lower awareness of risks, consequences, safeguards and their rights, additional emphasis was also placed on where such special protections were especially relevant (i.e. when children's data is processed for the purposes of marketing or creating personality or user profiles and the collection of children's data when using services offered directly to a child). The consent of a parent or legal guardian was omitted for preventive or counselling services offered directly to a child.

4.4. Article 8 of the GDPR as adopted

The official position of the Council was adopted on the 6th of April 2016 at first reading,[96] it was approved by the EP on the 14th of April 2016 in its second reading[97] and was finally adopted on the 27th of April 2016.[98] No definition of a child was included in the final text of the GDPR. As a consequence, a number of questions on how the rights, obligations and prohibitions contained in the GDPR (such as the right to erasure, obligations of data protection by design and default, transparent information, prohibition of profiling), related to children should be applied in terms of scope. It remains unclear whether they cover all children under 18 years old or different age limits (e.g. national age limits in analogy with Article 8), should apply. Article 8 retained its focus on the conditions applicable to children's consent in relation to information society services. An information Society Service is understood under the GPDR as 'a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the

Protection Regulation) [first reading] – Analysis of the final compromise text with a view to agreement, 15039/15, 15 December 2015 <http://data.consilium.europa.eu/doc/document/ST-15039-2015-INIT/en/pdf> accessed 10 April 2017.

[94]ibid.

[95]ibid.

[96]Council of the European Union, Position of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council 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), 5419/16, 6 April 2016 <http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf> accessed 10 April 2017.

[97]European Parliament, European Parliament legislative resolution of 14 April 2016 on the Council position at first reading with a view to the adoption of a regulation of the European Parliament and of the Council 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) (05419/1/2016 – C8-0140/2016 – 2012/0011(COD)) (Ordinary legislative procedure: second reading) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0125+0+DOC+XML+V0//EN> accessed 10 April 2017.

[98]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) [2016] OJ L119/1.

Council'[99] (Article 4(25) GDPR). The age limit of 16 was set as the rule for consent to the processing of personal data of a child, but this retained the possibility for Member States to use a lower age which could not go below 13 years. Recital 29 was renumbered to Recital 38 without however any substantial changes in its content. For the rest, Article 8 followed the amendments introduced in the draft of the 15th of June 2015, discussed above.

As a consequence, the adopted Article 8 of the GDPR left the existing state-of-the-art essentially unchanged: no coherent and uniform age threshold in the European Digital Market on when children can consent to their data processing themselves and to what extent their consent is valid. The remaining inconsistent age standards across the EU and between the EU and the US, not only undermines much-anticipated harmonisation effect of the GDPR, but also maintains significant challenges for companies that provide international services. Also, as noted by Kress and Nagel, the 'possibility to enact deviations could water down the level of protection which is initially awarded by Art. 8 GDPR'.[100] It is unclear whether Member States will act together to unify the age threshold in any way. At the time of writing, there have been discussions on lowering the age of consent to 13 years of age in at least two member states, the UK[101] and Belgium,[102] while the German draft for a new Federal Data Protection Act has retained the threshold of 16 years.[103]

From a policy making perspective, despite the efforts to promote the rights of the child in the EU policy making, the GDPR provision on the age of consent seems to be opaque, inconsistent and lacking explanations and evidence from the beginning. The EC originally did not have a strong position in relation to the protection of the personal data of children but changed its view on the age for parental consent during the revision process without clear justifications. Despite a number of amendments introduced by various members, the European Parliament avoided discussion of Article 8 choosing to focus its attention on other, more digital market related, articles. The Council has substantially deviated from the original EC proposal. It has initially increased the age limit of consent to 16 years and in the last minute of negotiations adopted a flexible approach leaving the decision partially to the Member states. Even more controversially, the EU was given a chance to re-affirm its commitment to protect the rights of the child in the information society, in the ePrivacy Regulation proposed on 10 January 2017[104] which is as a lex specialis to the GDPR (Article 1 I GDPR and recital 5 of the GDPR). It missed that opportunity, as the ePrivacy

[99]Directive (EU) 2015/1535 of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [2015] OJ L 241/1.

[100]Sonja Kress and Daniel Nagel, 'The GDPR and Its Magic Spells Protecting Little Princes and Princesses. Special regulations for the protection of children within the GDPR' (2017) 18(1) Computer Law Review International 6.

[101]James Titcomb, 'Britain Opts Out of EU Law Setting Social Media Age of Consent at 16', 16 December 2015 <http://www.telegraph.co.uk/technology/internet/12053858/Britain-opts-out-of-EU-law-raising-social-media-age-of-consent-to-16.html> accessed 3 March 2017.

[102]The Flemish Office of the Children''s Rights Commissioner, 'Advies bij General Data Protection Regulation van de EU, pleidooi sociale media vanaf 13 jaar', 2015–2016/09, 22 April 2016 <https://issuu.com/kinderrechten/docs/da6bbfb1-8a02-4d3f-9794-c31c0fd07d7a/1?e=6593254/36333697> accessed 3 March 2017.

[103]Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU), 18/11325, 24 February 2017 <http://dip21.bundestag.de/dip21/btd/18/113/1811325.pdf>.

[104]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 (ePrivacy Directive), Official Journal [2002] OJ L 201/37.

regulation neither continues the distinction between adults and children as data subjects nor refers to the specific requirements of Article 8 of the GDPR. Although it might be argued that protection of electronic communications can be generally addressed, a clear reference to the GDPR parental consent requirement would have been welcomed[105] and demonstrate consistency and commitment to the purpose of protecting children online.

5. The US COPPA and parental consent

Introduced more than 15 years ago in the US, the COPPA[106] is one of the first pieces of legislation adopted to specifically protect the privacy of minors under 13 years of age online. Although not entirely uncontroversial, COPPA 'seeks to put parents in control of what information commercial websites collect from their children online'.[107] It has been considered by the FTC, COPPA's primary enforcer, as an effective act protecting children without unduly burdening operators of online services,[108] but heavily criticised by others due to its limited scope (children below the age of 13), the burden of parental consent mechanisms for service operators, the possible impact on online anonymity, and the balance between parental and service provider responsibility.[109]

As a general rule, COPPA requires online services that are directed towards children or that have actual knowledge that they have users under 13 (e.g. because the service collects date of birth) to obtain verifiable parental consent before collecting any personal information. COPPA applies only to commercial service providers and non-profit entities generally are not covered by the parental consent requirement.

Under COPPA, 'verifiable parental consent' means that the consent method must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent. The FTC specifies several possible methods of obtaining verifiable consent, if children's personal information is going to be disclosed to third parties (except service providers) or made publicly available online, such as in a chat, profile or similar feature. These include, for example:

- providing a form the parent can print, fill out, sign and post, fax or scan and email back;
- requiring the parent to use a credit card or similar method of payment (such as PayPal) in connection with a monetary transaction (this could include a membership or subscription fee, or simply a charge to cover the processing of the card);
- maintaining a free-phone (toll free) number staffed by trained personnel for parents to call in their consent;
- permitting the parent to connect to trained personnel via video conference; or
- verifying the parent's identity by checking a form of government-issued ID against a database of such information, provided that the ID is deleted promptly after verification is complete.

[105]Kress and Nagel (n 100) 6.
[106]Children''s Online Privacy Protection Act 1998, 15 U.S.C. 6501–6505.
[107]FTC, 'Children''s Online Privacy Protection Rule: Not Just for Kids' Sites' <https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-not-just-kids-sites> accessed 3 March 2017.
[108]FTC, 'Implementing the Children's Online Privacy Protection Act: A Report to Congress', February 2007 <http://www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf> accessed 3 March 2017.
[109]Chris J Hoofnagle, *Federal Trade Commission Privacy Law and Policy* (CUP, 2016), 208 (he provides an overview of critique for COPPA as a privacy measure).

In cases where the information is not going to be disclosed or made publicly available, an additional method known as 'email-plus' is allowed. This method involves the service operator's obtaining consent through the receipt of an email from the parent, plus one further step: the service provider can contact directly the parent using a postal address, telephone or fax, or send another email to the parent to confirm their consent.

COPPA foresees certain exceptions to the general consent rule. Verifiable consent is not needed when: (1) responding to a one-time request from a child, provided that the child's personal information is deleted after the response is made; (2) collecting personal information in order to send the child periodic communications such as newsletters, provided that the parent is given the opportunity to opt out; (3) where necessary to protect the safety of a child participating in the service; or (4) where necessary to protect the security/integrity of the service, respond to a judicial request or other public investigation.

In practice, most child-directed online services appear to operate under one of the exceptions to COPPA that allows a one-time use, multiple online contact with simply a notice to a parent (and opportunity to opt out), or e-mail plus.[110] This limited use of legal COPPA provisions can be claimed to demonstrate the reluctance among industry to fully embrace COPPA in their services.

Contrary to the child-specific services, general audience sites and services do not have to obtain parental consent unless they have actual knowledge that their users are under 13. In practice, this means that many general audience services expose themselves to COPPA only if they collect age or date of birth. As a result, for them to avoid having to comply with COPPA (i.e. to avoid acquiring actual knowledge that a user is a child) it is simply sufficient to avoid the collection of the age or the date of birth of users. In contrast, although general audience sites and services do not have an obligation to collect age information, some service providers take precautions by explicitly prohibiting the users under 13 from using the service in the terms and conditions and asking all users to enter their birth date before they can access the service. In accordance with the FTC's suggestion, they ask for the age in a neutral manner, that is, allowing any birth date to be entered without stating or implying that a user has to be at least 13. If the date given proves users to be under 13, they age gate and block them. In addition, a cookie can be placed on their computer preventing them from simply re-entering false information.

From the 1st of July 2013 the FTC amended COPPA in order to clarify its scope and strengthen protection for children's personal information (i.e. 'to minimise the collection of personal information from children and create a safer, more secure online experience for them') in light of changes in online technology and the evolving use of such technologies by children since COPPA first went into effect in April 2000.[111] The amendments include modifications to the definitions of operator, personal information, and Web site or online service directed to children. It also updated the requirements set forth in the notice, parental consent, confidentiality and security, and safe harbour provisions, and added a new provision addressing data retention and deletion.

[110]Advertising Education Forum, 'Children's Data Protection and Parental Consent: A Best Practice Analysis to Inform the EU Data Protection Reform', October 2013 <http://www.aeforum.org/gallery/5248813.pdf> accessed 10 April 2017, 18.
[111]FTC, Children's Online Privacy Protection Rule, Final rule amendments, 78(12) Fed. Reg. 3972, 17 January, 2013.

6. Understanding parental consent in practice

As Article 8 of the GDPR is without precedent in Europe, its practical implementation raises many questions, such as to which services the requirement will apply, how child directed services will be delineated, and how consent and age should be verified. These questions will need to be addressed by the national legislators, DPAs and the EDPB where relevant in the future. In this part we will therefore discuss the key uncertainties that merit attention before the GDPR comes into effect.

6.1. Information society services

The general GDPR provisions apply to any service that involves personal data processing, wholly or partly by automated means or when personal data form part of a filing system (Article 2 GDPR). Article 3 explicitly specifies that it applies to free services offered to data subjects in the EU by a controller or processor not established in the EU territory.[112] To the contrary, the parental consent requirement, that is, Article 8 GDPR, has a specific material scope and is applicable to the information society services offered directly to a child. To define the meaning of the specific scope of application of Article 8, the GDPR makes use of the definition of an information society service contained in Directive (EU) 2015/1535 which defines such services as 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services' (Point (b) of Article 1(1) Dir. 2015/1535).[113] The notion of 'remuneration' under this definition could be interpreted in a very restrictive way, requiring the user to pay for the provided service. However the majority of the services offered in the information society do not directly require remuneration from the users, including free social media, online gaming, entertainment sites, email or instant messaging services. Therefore, the phrase 'normally provided for remuneration', should be interpreted broadly. The European Court of Justice has dealt with the concept of remuneration in the context of services offered within the EU in various cases and has adopted such an interpretation. In Belgium v Humbel the European Court of Justice considered that 'the essential characteristic of remuneration […] lies in the fact that it constitutes consideration for the service in question and is normally agreed upon between the provider and the recipient of the service'.[114] It is not the recipient who necessarily gives the remuneration; the critical

[112]Article 3 states: 'Territorial scope:
(1) This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
(2) This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
(b) the monitoring of their behaviour as far as their behaviour takes place within the Union'.

[113]In contrast, the US COPPA does not mention the distinction between free and paid online services, and applies to operators of child-directed websites and online services collecting personal information, broadly covering 'any service available over the Internet, or that connects to the Internet or a wide-area network'. According to the FTC, 'examples of online services include services that allow users to play network-connected games, engage in social networking activities, purchase goods or services online, receive online advertisements, or interact with other online content or services. Mobile applications that connect to the Internet, Internet-enabled gaming platforms, voice-over-Internet protocol services, and Internet-enabled location-based services also are online services covered by COPPA'. See FTC, 'Complying with COPPA: Frequently Asked Questions', Section A. Question 9. <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General%20Audience> accessed 3 March 2017.

element is that the remuneration is given to the provider of the service. Indeed in Bond van Adverteerders v Netherlands, the Court of Justice of the EU found that the remuneration does not need to come from the recipient of the service (i.e. in this case the viewer), instead it suffices that the remuneration comes from another party, such as an advertiser.[115] The Court of Justice of the EU has further ruled that a service can be considered as provided for remuneration even in cases where the provider is a non-profit organisation, when there is an 'element of chance' inherent in the return or when the service is of recreational or sporting nature, within this interpretation.[116] Therefore, an activity that is financed via advertising can also be considered as being provided for remuneration, even if the remuneration does not come directly from the user.[117] This interpretation is also in line with the original idea of the EC to protect children on social networks[118] and with the understanding of Article 8 of the GDPR by the Bavarian DPA.[119]

As a result of the broad interpretation of the term 'information society services', the GDPR parental consent requirement will be potentially applicable to a very wide range of online services. The only clear precondition is that personal data is processed by the service and consent is the legal grounds on which this processing is based. Hypothetically, it can be questioned whether any online services offered directly to children can remain outside the parental consent requirement, given the fact that even though there are many websites that can be used without actively providing personal data, such as news or entertainment websites, personal data is often passively collected through tracking techniques (i.e. browser fingerprinting or cookies) and requires users' consent under the e-Privacy Directive.[120]

Such a potential over-reliance on parental consent to process children's personal data is hardly desirable, given the deficiencies of consent as a protection mechanism and possible unintended consequences, such as 'consent fatigue' among parents, and potential limitation of children's rights and opportunities (discussed below). Instead of consent, it is worth considering if other lawful grounds such as 'legitimate interests' of data controllers (Article 6.1(f) GDPR) could allow to better safeguard the righs of children and ensure a closer scrutiny when personal data of children is processed, if they are complemented with stricter audits and data compliance mechanisms. In fact, the UK ICO encourages data controllers to rely on the legitimate interest ground, because before invoking it they need to assess the impact of their data processing on children, and consider if

[114]C-263/86 *Belgian State v René Humbel and Marie-Thérèse Edel (Belgium v Humbel)* [1988] ECR 5365, para 17.

[115]C-352/85 *Bond van Adverteerders v Netherlands State* [1988] ECR 2085. Paul Craig and Gráinne de Búrca, *EU Law – Text, Cases, and Materials* (4th edn Oxford University Press, Oxford, 2008), 819.

[116]Craig and de Búrca (n 115) (provide extensive references to various cases of the Court of Justice relating to the concept of services and remuneration). See for instance: C-70/95 *Sodemare and others/Regione Lombardia (Sodemare)* [1997] ECR I-3395; C-275/92 *H.M. Customs and Excise/Schindler (Schindler)* [1994] ECR I-1039; C-415/93 *Union royale belge des sociétés de football association and others/Bosman and others (Bosman)* [1995] ECR I-4921.

[117]Robert Queck and others, 'The EU Regulatory Framework Applicable to Electronic Communications' in Laurent Garzaniti and Matthew O'Regan (eds), *Telecommunications, Broadcasting and the Internet – EU Competition Law & Regulation* (3rd edn Sweet & Maxwell, 2010), para 1-047.

[118]EC confirmed that he main objective of Article 8 is to protect children on social networks. See Council of the European Union, Note from Presidency to Working Party on Information Exchange and Data Protection, 11028/14, 30 June 2014, 87–88.

[119]Bavarian Data Protection Authority, 'Information sheet for the implementation of the GDPR, No. 15', 20 January 2017 <https://www.lda.bayern.de/media/baylda_ds-gvo_15_childs_consent.pdf> accessed 3 April 2017.

[120]Article 5(3) of the ePrivacy Directive requires prior informed opt-in consent for storage and access to information on users' terminal equipment.

such processing is fair and proportionate.[121] In the same vein, due to a high possibility to gain ill-informed consent and the subsequent complications in withdrawing such an invalid consent, some DPAs advise against the use of consent of children or do not recognise consent given by them to legitimise data processing operations.[122]

If data controllers fully consider all the factors (e.g. the nature and source of the legitimate interest, the aim of the data processing, the impact on children and their reasonable expectations, additional safeguards to limit undue impact on children) and ensure that the interests and fundamental rights of children are duly taken into account,[123] the legitimate interest ground can potentially protect children more than the reliance on consent. Even more so, because in case of children the interpretation of the legitimate interest grounds is restricted by the GDPR. Due to the special status of children as data subjects their rights should be considered as overriding the legitimate interest of the data controllers more easily than adult's rights (Article 6.1(f) GDPR).

6.2. Services offered directly to children

The GDPR parental consent requirement concerns online services offered directly to children. Although the intention of the legislator to create a specific protection regime for services that process children's personal data is clear, the exact distinction of services to which the protection applies is a complex issue. In practice, services targeted at children compose only a small part of all services that children can access, use, and sign up to. The latter, so called general and mixed audience services, generate major privacy concerns and anxieties in practice. Various studies in Europe[124] and North America[125] report that from a broad range of websites that children use nowadays, the most popular websites (such as YouTube, Facebook and Google search to name just a few) are often not directed specifically to children (at least not those under 13). Many of such websites claim in their terms of use that their services are not intended for those under 13, even if in practice substantive numbers of young children are in fact active users.[126] As a result, the young 'unauthorised users' are treated as adults and presented with the same information and privacy settings, without any consideration of their particular needs, online behaviour or the risks for them in the online environment. Thus, an important question is to what extent the GDPR will reflect reality and to what extent the parental consent requirement will cover general-audience or mixed-audience services and sites?

[121]UK Information Commissioner's Office (UK ICO), 'Consultation GDPR consent guidance', March 2017 <https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf> accessed 8 April 2017.

[122]Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (OUP, 2007) 211.

[123]Article 29 Working Party, 'Opinion 06/2014 on the Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP217', 9 April 2014.

[124]Sonia Livingstone and others, 'Risks and Safety on the Internet: The Perspective of European Children' (LSE, EU Kids Online, London 2011).

[125]Valerie Steeves, 'Young Canadians in a Wired World, Phase III: Life Online' (MediaSmarts, Ottawa 2014).

[126]Courtney K Blackwell and others, '*Children and the Internet: Developmental Implications of Web Site Preferences among 8- to 12-Year-Old Children*' (2014) 58(1) Journal of Broadcasting & Electronic Media, 1 (data collected from 442 8- to 12-year-old US children to investigate their Internet content preferences indicated that YouTube (26%) and Facebook (18%) were the two most favoured websites in this age group). danah boyd and others, 'Why Parents Help Their Children Lie to Facebook about Age: Unintended Consequences of the 'Children's Online Privacy Protection Act' (2011) 16(11) First Monday (surveyed 1007 US parents or guardians with children ages 10–14 and found that 19% of 10-year-olds, 32% of 11-year-olds and 55% of 12-year-olds have a Facebook account). Sonia Livingstone and others, 'Risks and Safety on the Internet: The Perspective of European Children' (LSE, EU Kids Online, London 2011) (surveyed 25,142 9- to 16-year-olds in 25 EU countries and showed that 38% of 9- to 12-year-olds have their own profile on social networks).

As the GDPR has just been adopted, the answer to this question is unclear. The FTC under COPPA in the US has indicated several criteria to determine whether a website or an online service is directed at children. These criteria include: the subject matter of the service, its visual content, the use of animated characters or child-oriented activities and incentives, music or other audio content, the age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the website or online service, or whether advertising promoting or appearing on the website or online service is directed to children.[127] Competent and reliable empirical evidence of audience composition and evidence regarding the intended audience are also among the factors to be considered.[128] This 'totality of the circumstances test'[129] seems a solid yardstick if applied holistically,[130] but might prove problematic if taken in parts. For example, in 2014 the FTC brought a case against TinyCo, deciding that their fantasy apps were subject to the COPPA requirements based mainly on the appearance of these apps'. The FTC claimed that

> apps appeal to children by containing brightly-colored, animated characters from little animals or zoo creatures to tiny monsters, and by involving subject matters such as a zoo, tree house, or resort inspired by a fairy tale [and] the language used to describe the apps in the app stores and the gameplay language is simple and would be easy for a child under age 13 to understand.[131]

As Hoofnagle noted, 'many general-audience apps have childish themes'.[132] This can be well illustrated by the Angry Birds app, which entails child appealing, animated characters, such as stylised colourful wingless birds and green pigs, and thus seems to meet the FTC's criteria for being directed at children, but in fact is widely used by adults in practice.[133]

The FTC has found a solution which, although not entirely uncontested, partially subjects general audience services (i.e. services that are not targeting children but are used by them) to COPPA requirements. It uses the 'actual knowledge' test, according to which the COPPA obligations apply to operators of general online services that have actual knowledge that they are collecting, using or disclosing the personal information of children. The general service providers are not obliged to investigate the age of their users actively, but acquiring passive knowledge of children using the service creates obligations under COPPA. Such passive knowledge can be gained, for example, if the operator learns that the person is a child under 13 when dealing with its users, such as responding to an email, seeing the age or the grade in a feedback option, or getting to know the age from a concerned parent, or if a child announces their age in a post seen by an employee of the operator.[134] The actual knowledge standard seems to be problematic in its

[127]FTC, 'Complying with COPPA: Frequently Asked Questions'<https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General%20Audience> accessed 1 March 2017.
[128]16 C.F.R. §312.2. See also FTC, 'Implementing the Children's Online Privacy Protection Act: A Report to Congress' (February 2007) <http://www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf> accessed 3 March 2017.
[129]Hoofnagle (n 109) 200.
[130]The COPPA Rule's Statement of Basis and Purpose (64 Fed. Reg. 59893) states that the FTC, in making its assessment, should consider 'the overall character of the site – and not just the presence or absence of one or more factors'.
[131]*US v Tinyco.inc* 2014.
[132]Hoofnagle (n 109) 200.
[133]Paul Sawers, 'Nielsen Reveals Most Popular Android Apps by Age. Angry Birds Appeals Most to over 35s', 12 December 2011 <https://thenextweb.com/google/2011/12/12/nielsen-reveals-most-popular-android-apps-by-age-angry-birds-appeals-most-to-over-35s/> accessed 5 March 2017.
[134]FTC, 'Complying with COPPA: Frequently Asked Questions'.

applicability, as not having actual knowledge of underage service users seems easy to prove, and the standard encourages service provider ignorance as a means of avoiding compliance. The standard is likely to be met if a child announces their age in a post and the provider monitors the posts, but if the provider does not engage in monitoring, it could be assumed that no one in the organisation is aware of the post. The actual knowledge standard has been applied by the FTC in several cases to operators that had age screening in place but allowed children under the age of 13 to register.[135]

The FTC also has a solution for addressing the issue of COPPA applicability to the services that target mixed audiences, such as teenagers under and above 13 or both adults and children. As a general rule, if a service targets children under 13 as one of its audiences (even if not as its primary audience), it is considered to be 'directed to children'. However, to avoid COPPA applicability to all users in mixed audience services, the amended COPPA Rule foresees a narrow possibility to employ an age screen in order to identify children under 13 and provide COPPA protection only to them. After identifying the users under 13, service providers can choose to either collect parents' online contact information and obtain parental consent or prevent the collection of personal information from these users (e.g. direct them to content that does not collect, use, disclose personal data). Services directed wholly or primarily to children, in contrast to services directed to the users over 13, cannot use the above-mentioned age screen to block children under the age of 13 because of their very nature. According to the FTC, in most cases, a service directed to children must consider all visitors as children without screening them for age and provide to all of them COPPA's protection.

Taking into account the empirical evidence on children's wide use of general-audience services and extensive direct marketing and profiling carried out by these services, it is hard to imagine that the GDPR could not extend the protection to children using these services. The first emerging opinions consider general-audience services, such as Facebook, WhatsApp or Instagram, to fall under the scope of Article 8 of the GDPR.[136] The next challenging task for the EDPB and national DPAs will be to crystallise the approach on this distinction and to specify related obligations. One of the possible options could be taking a much more protective and rigid approach than the US in COPPA and instead of allowing a simple age screening and blocking users under the established age (in the 13–16 age span) in mixed audience services, the GDPR could require appropriate and adequate age verification of users (as discussed below) and protection of those who are under the established age.[137] Such protection would ideally include no or minimal data collection and no disclosure of personal data to third parties – but still provision of interactive and interesting services – or otherwise, if personal data is collected, at

[135] *US v Yelp.inc* 2014, *US v Path* 2013; *US v Artist Arena* 2009, *US v Sony* 2008; *US v Xanga.com*; *Us v UMG Recordings.inc* 2004.

[136] Bavarian Data Protection Authority, 'Information Sheet for the Implementation of the GDPR, No. 15', 20 January 2017; Kress and Nagel (n 100).

[137] A similar proposal is provided by Karen Mc Cullagh in the context of social networks (SNSs), who claims that 'it would have been better to encourage children to provide their true age to SNSs and require SNSs to offer alternative, child-friendly services. This could have been done, for example, by offering platforms to facilitate expression and socialisation by children and permit SNSs to collect performance data from children without parental permission so as to enhance the service offered, but mandate that no profiling and tracking of children's data can be conducted for commercial purposes' (Karen Mc Cullagh, 'The General Data Protection Regulation: a partial success for children on social network sites?', in Tobias Bräutigam and Samuli Miettinen (eds) *Data Protection, Privacy And European Regulation in the Digital Age* (Unigrafia, Helsinki, 2016) 129–130).

least a verifiable parental consent or reliance other carefully considered legitimate ground, prohibition of profiling and marketing, and age-adapted information.

6.3. Consent authorised by the holder of parental responsibility

Article 8 of the GDPR allows consent not only to be given by the holders of parental responsibility over the child but also for the consent to be authorised by them. From the final text of the GDPR, it remains unclear if and under what circumstances parents are allowed to authorise the consent already provided by the child or other individuals on behalf of the child. In this respect, two questions arise: Could the reference to consent authorisation be understood as allowing a joint consent, that is, a possibility for parents to approve post factum the consent of a child in specific circumstances? Could the circle of holders of parental responsibility include individuals other than parents and legal guardians?

Consent authorisation is not used as a general or child-specific practice under Directive 95/46/EC. It remains to be seen what weight and under what conditions the consent authorisation mechanism will be afforded by the national legislators, the DPAs and the EDPB in the context of the GDPR. If acknowledged and interpreted broadly, the consent authorisation option can allow the parallel or joint consent of the child and a parent,[138] and thus provide for a more flexible parental consent procedure than is currently explicitly acknowledged in the GDPR. Alternatively, Article 8 will continue to be interpreted as an over protective and fully applicable (except in preventive or counselling services) requirement, that risks limiting children in their online freedoms and opportunities.[139]

The second question relates to the flexibility of the GDPR parental consent requirement to accommodate a wider circle of competent individuals in the definition of the term 'holders of parental responsibility'. Some national laws affords such flexibility, for example the Irish data protection law allows a grandparent, uncle, aunt, brother or sister of the data subject to consent on their behalf, when the giving of such consent is not prohibited by law.[140] In Malta, the national data protection law not only allows individuals acting in loco parentis but also those acting in a professional capacity in relation to a child to process personal information without necessarily involving parents, if such processing is in the best interest of the child.[141] Similarly, in the US schools may act on

[138]Article 29 Working Party, 'Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools) WP 160', 11 February 2009.

[139]Milda Macenaite, 'From Universal Towards Child-Specific Protection of the Right to Privacy Online: Dilemmas in the EU General Data Protection Regulation' (2017) 19(5) New Media and Society 765.

[140]Data Protection Act 1988 (updated 14 October 2014) (Article 2A states:

> (1) Personal data shall not be processed by a data controller unless […] at least one of the following conditions is met:
> (a) the data subject has given his or her consent to the processing or, if the data subject, by reason of his or her physical or mental incapacity or age, is or is likely to be unable to appreciate the nature and effect of such consent, it is given by a parent or guardian or a grandparent, uncle, aunt, brother or sister of the data subject and the giving of such consent is not prohibited by law).

[141]Subsidiary legislation 440.04 Processing of personal data (protection of minors) regulations, 12 March 2004. (the law states: 2.(1) Where any information is derived by any teacher, member of a school administration, or any other person acting in loco parentis or in a professional capacity in relation to a minor, such information may be processed by any of the aforesaid persons if such processing is in the best interest of the minor. (2) Where personal data is being processed as aforesaid, the consent by the parents or other legal guardian of the minor shall not be required if

the parents' behalf in the educational context when personal data is collected from students for the use and benefit of the school, but not for other commercial purposes.[142] In this case, it can be presumed that the school's authorisation for data collection is based on the parental consent obtained by the school and that a direct parental consent is not required. In order to understand the GDPR in this respect, the interpretation of the 'holder of parental responsibility' notion should be aligned with the family law.[143] The concept 'parental responsibility' refers to the duties and rights to take care of the child's person (ensure shelter, food and clothes, represent legally, responsibility for the child's upbringing) and look after the child's property. The persons having the parental responsibility of a child are the 'holders of parental responsibility', most often being the parents. Nevertheless, if the parents are deceased, not capable or authorised to take care of their child, a guardian such as a relative, a third person or an institution, can be appointed by court to represent the child. Following this definition, the circle of competent persons to provide consent under Article 8 of the GDPR is limited to parents and legal guardians. Thus, if not appointed by the court, it cannot include a wider circle of relatives or expand beyond parents to the professionals working with children. Although inflexible, the choice to limit competent persons to provide parental consent is understandable. Consent in the GDPR is just one of several grounds for data processing and other legal grounds such as compliance with a legal obligation, the performance of a task carried out in the public interest or in the exercise of official authority or legitimate interest of the data controller can also be applicable to the processing of children's personal data by individuals acting in their professional capacity in relation to children, such as teachers in schools. In addition, the parental consent requirement in Article 8 only relates to online services and thus offline data collection from children is subject to general GDPR consent requirements and the relevant national legislation. Parental consent can still be required in relation to offline collection of personal data of children, when this is so required in accordance with national legislation or when children lack the legal capacity to provide valid consent.

6.4. Verifiable and verified consent

The original Commission Proposal required parental consent to be verifiable by stating: 'the controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology' (Article 8(1) EC proposal). The final text of the GDPR, however, adopted a different wording and refers to the effort that data controllers should make to verify parental consent. It states that 'The controller shall make reasonable efforts to verify […] that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology'

this may be prejudicial to the best interest of the minor. (3) In such a case, no parent or other legal guardian of the minor shall have access to any personal data held in relation to such minor.)

[142]FTC, 'A Guide for Business and Parents and Small Entity Compliance Guide' <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions> accessed 1 April 2017.

[143]The term 'parental responsibility' and all rights and duties of a holder of parental responsibility relating to the person or the property of the child in the EU is defined in Article 1(2) of the Council Regulation (EC) No 2201/2003 of 27 November 2003 concerning jurisdiction and the recognition and enforcement of judgments in matrimonial matters and the matters of parental responsibility, repealing Regulation (EC) No 1347/2000 [2003] OJ L 338/1. See also European Commission, 'Practice Guide for the Application of the Brussels IIa Regulation' <http://ec.europa.eu/justice/civil/files/brussels_ii_practice_guide_en.pdf> accessed 1 March 2017.

(Article 8(2) GDPR). This change may have different implications for data controllers. While the duty to make reasonable efforts to 'verify' consent refers to a one time parental consent verification (i.e. a single verification moment) which should take place prior to the collection of children's personal data, the duty to obtain 'verifiable' consent calls for consent to be verifiable at any time (i.e. an ongoing possibility of re-verifying). Even more importantly, the change from 'verifiable consent' to 'verify consent' means a lower burden on data controllers providing child-directed services online. A reference to 'verifiable consent' would have meant that consent could not have been given if it could not be verified and that data controllers should ensure verification through technological means or abstain from relying on consent. The requirement to make reasonable efforts to verify consent is different as it allows the data controller to show that reasonable efforts were made to verify consent and, in circumstances where this was not possible, the data controller may still rely on the unverified consent to process children's data.

The GDPR parental consent requirement is a flexible liability standard. To be compliant, it suffices to make reasonable efforts to obtain verifiable parental consent rather than necessarily obtaining it in all cases. The reference to 'reasonable efforts' alludes to the fact that data controllers cannot guarantee verified consent as a final outcome that has to be achieved under the GDPR be that due to a situation beyond their control or due to uncertainty surrounding the technological consent verification capabilities. In the former case, it is not clear how much effort and proof in relation to obtaining consent can be requested from the controllers in situations where it is difficult to acquire verifiable parental consent, for example where discovering the whereabouts or contact information of the parents proves challenging or when the rights of the parents over the child have been terminated and the other legal representative of the child are difficult to reach. How much effort to reach a parent or a legal guardian should be sufficient to demonstrate compliance? How should the exercise of the reasonable efforts be documented and proven? By relying on the reasonable efforts yardstick the burden of proof to demonstrate that a valid consent has been obtained is problematically weakened.[144] In the latter case, data controllers are left with the discretion to choose solutions for obtaining parental consent, taking into account available technology, which might not always be foolproof or lead to very high costs in implementation. If the data controller does not attain parental consent, but still processes the personal data of children, it is important to know how to evaluate if the efforts were reasonable, and establish clear guidelines when less reliable consent verification tools are considered sufficient and how consent verification costs and benefits can be weighted. Otherwise, there is a risk that the vagueness of the reasonable efforts standard can become a shield for the wilful breach or disregard of the parental consent requirement. As the GDPR fails to provide a definition for 'reasonable efforts', it is likely that the DPAs and the courts will look into the specific facts and circumstances of the case, examine the controller's efforts and the extent of technological capabilities to obtain verifiable parental consent.

[144]Hornung Gerrit, 'A General Data Protection Regulation for Europe: Light and Shade in the Commission''s Draft of 25 January 2012' (2012) 9 SCRIPTed 64.

6.5. Consent verification

The GDPR establishes a general requirement to verify parental consent taking into account available technology. Specific parental consent mechanisms that can be used by data controllers to be compliant with the GDPR are not specified and will require further clarification. Lack of clarity on specific methods can lead to GDPR infringements that can attract an administrative fine of up to 2% of total global annual turnover or 10 000 000 EUR (Article 83.4).

Similar to the FTC in the US, the EU should specify the possible parental consent methods that are considered to be acceptable in light of available technology to ensure that the person providing consent is the child's parent. The FTC has established a number of acceptable methods for attaining parental consent in order to provide a clear set of choices for industry. It also allows interested parties to submit new verifiable parental consent methods to the FTC for approval. The aim of this provision is to encourage the development of new consent verification methods that are effective but also acceptable for industry and can be used by the applicant or any other party. After the adoption of the amended COPPA rule, the FTC received a number of requests to approve industry proposed verifiable consent methods, thus showing an unprecedented boost in this sector.

In November 2013, the FTC received an application seeking approval of a 'social-graph verification' mechanism, a verifiable parental consent method submitted by AssertID, Inc.[145] The proposed method would ask a parent's 'friends' on a social network to verify the identity of the parent and the parent-child relationship. In a letter to AssertID, the FTC noted that the company's proposal failed to provide sufficient evidence that its method would meet the requirements set out under the COPPA rule. Specifically, the FTC considered the approval of this method under the COPPA Rule as premature, noting that there was not yet adequate research or market testing to show the effectiveness of the 'social-graph verification' method.[146] Thus such a method cannot ensure that the person providing consent is the child's parent.

In December 2013, based on an application submitted by Imperium, Inc., the FTC approved the use of knowledge-based authentication as a method to verify that the person providing consent for a child to use an online service is in fact the child's parent.[147] Knowledge-based identification is a way to verify the identity of a user by asking a series of challenge questions, typically that rely on so-called 'out-of-wallet' information; that is, information that cannot be determined by looking at an individual's wallet and are difficult for someone other than the individual to answer. This authentication method has been used by financial institutions and credit bureaus for a number of years, and has been acknowledged by the FTC and other government agencies as effective for that purpose.

[145]FTC, 'Letter to AssertID', 12 November 2013 <https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-denies-assertids-application-proposed-coppa-verifiable-parental-consent-method/131113assertid.pdf> accessed 1 March 2017.
[146]ibid.
[147]FTC, 'Letter to Imperium, 23 December 2013' <https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-grants-approval-new-coppa-verifiable-parental-consent-method/131223imperiumcoppa-app.pdf> accessed 1 March 2017.

In January 2015, the FTC denied the AgeCheq proposed method, a device-signed parental consent form to obtain verifiable parental consent. It was a multi-step method requiring the entry of a code sent by text message to a mobile device. The FTC decided that the company's proposed mechanism was not compliant with COPPA's requirements regarding the type of parental information that can be collected as a means to verify a parent's identity. The AgeCheq's method did not meet the COPPA requirement of a reasonably calculated age verification method to ensure that the person providing consent is the child's parent or guardian as the person providing consent could easily be the child using the very device on which an app seeking consent was downloaded.[148]

6.6. Verification of age

The GDPR requires that the data controllers obtain verifiable parental consent before processing personal data of children, but there is no particular requirement to authenticate the age of the child, that is, to verify that the data subject is of a certain age or belong to a certain age group. This is the case despite the fact there have been calls to include the rules on adequate age verification into the GDPR.[149] The initial proposal of the EC provided for delegated acts on this issue, but this proposed provision did not make into the final text of the GDPR.

Age verification may not be necessary for services that by default focus on very young children (i.e. those under 13) which a priori require parental consent from all the users. However, for services targeting teens, mixed audiences or general audience services that are also used by children, in order to fully comply with the GDPR parental consent requirement a service provider needs to know which users are legally competent to consent and from whom parental consent should be sought.

The fact that the GDPR does not refer to age verification is not surprising per se. First, the topic of age verification still raises many sensitive and unresolved questions related to online anonymity, freedom of speech and expression, and privacy vis-à-vis both children and adults online.[150] The idea that all internet users in general audience websites could be asked to provide their age or even worse to identify themselves might not only lead to increased personal data gathering but may also be viewed as disproportionate and thus

[148]FTC, 'Letter to AgeCheq Inc.', 27 January 2015 <https://www.ftc.gov/system/files/documents/public_statements/621461/150129agecheqltr.pdf> accessed 1 March 2017.

[149]The Article 29 Data Protection Working Party repeatedly stressed the importance of adequate age verification. In the 'Opinion 15/2011 on the definition of consent, WP 187' it advocated age verification use and advised to include into the revised Directive 95/46/EC specific provisions on age verification. As an example it proposed to establish age verification on 'sliding scale approach' which would mean that age verification mechanisms depend on the specific circumstances relating to the specific data processing operation, such as the types of personal data that will be processed, the purposes for which they will be processed, eventual risks arising from the processing etc. Equally, Article 29 Data Protection Working Party, in its Opinion 5/2009 on online social networking, WP 163 (12 June 2009, 12) stated: 'The Working Party encourages further research on how to address the difficulties surrounding adequate age verification and proof of informed consent in order to better address these challenges'.

The European Data Protection Supervisor also claimed: 'If parental consent is necessary, it would be necessary to establish rules on how to authenticate the age of the child, in other words, how to know that the child is a minor and how to verify parental consent' (Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – 'A comprehensive approach on personal data protection in the European Union', 22 June 2011).

[150]Berin Michael Szoka and Adam D Thierer, 'COPPA 2.0: The New Battle Over Privacy, Age Verification, Online Safety & Free Speech' Progress & Freedom Foundation Progress on Point Paper No. 16.11, May 21, 2009; Adam D Thierer, 'Social Networking and Age Verification: Many Hard Questions; No Easy Solutions', Progress & Freedom Foundation Progress on Point Paper No. 14.5, March 2007.

simply unacceptable. Second, although age verification has been already widely used as a regulatory solution across Europe in online gambling or online sales of age-restricted goods (alcohols, tobacco, etc.), in these sectors there is extensive evidence related to potential risks and harms associated with the use of such restricted goods and services by minors.[151] It is not the case with privacy and data protection risks and harms, which still lack a detailed and convincing evidence database. The privacy risk and harm assessments debate is still in its embryonic phase[152] and as of yet there is no consensus around what constitutes a privacy harm. Regulators and companies have equally failed to identify a comprehensive list of privacy harms and negative impacts on data subjects.[153,154] Third, some of the existing age verification solutions are not suitable in the data protection context, which requires a granular, more complex approach than verifying that a person is an adult (18 and above). Age verification, as a means of distinguishing between individuals under and over 18, has been used by service providers for controlling access to harmful content, such as offensive or sexually explicit, online content,[155] through the implementation of the Audiovisual Media Service Directive.[156] In practice, unsuitable content is concealed behind a 'pay wall' which can be passed by payment methods which are restricted to adults (such as payment by credit card) or age can be established using an independent and reliable database, such as the electoral roll.[157] None of these methods are appropriate for the implementation of the GDPR, as the age thresholds (13–16) are various and do not coincide with the legal majority age of 18. This means that there are a limited number of reliable databases on age data for minors, as the majority of the databases (social security number, passport number) only demonstrate that an individual is an adult, without any possibility, at least in their current form, of obtaining granularity in terms of age.[158] Also, the availability of datasets differ from country to country, as for example, in Denmark and Belgium there are more extensive databases on children that could be used. Crosschecking in public databases is reliable and trustworthy, but complex to implement and pose huge privacy concerns because of the sensitivity of the data being processed.

[151]Victoria Nash and others, 'Effective Age Verification Techniques: Lessons to be learnt from the online gambling industry' (Final Report) (2014), Oxford Internet Institute, University of Oxford.

[152]M Ryan Calo, 'The Boundaries of Privacy Harm' (2011) 86 Ind. L.J. 1131; David Wright and Charles Raab, 'Privacy Principles, risks and harm' (2014) 28(3) International Review of Law, Computers & Technology 277.

[153]National Institute of Standards and Technology, NIST Privacy Engineering Objectives and Risk Model (Discussion Draft) (2014), 3. Some efforts to articulate privacy harms, include: Centre for Information Policy Leadership at Hunton &Williams LLP, 'A Risk-Based Approach to Privacy: Improving Effectiveness in Practice' (2014) and 'The Role of Risk Management in Data Protection' (2014).

[154]Nash and others (n 151) 2.

[155]Recommendation 2006/952/EC of the European Parliament and of the Council of 20 December 2006 on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and on-line information services industry [2006] OJ L 378/72, paras II 1, 2.

[156]Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) [2010] OJ L95/1.

[157]The UK regulatory bodies, especially the Authority for Television on Demand (ATVOD), has paved the way within the EU in strengthening the protection of minors in on-demand services and enforcing the 'effective Content Access Control System ("CAC System")' 'which verifies that the user is aged 18 or over at the point of registration or access' of the service. See ATVOD, 'Rules & Guidance, Statutory Rules and Non-Binding Guidance for Providers of On-Demand Programme Services (ODPS)', Edition 2.1, Rule 11, 13; ATVOD, 'For Adults Only? Underage Access to Online Porn', 28 March 2014, 7–9.

[158]Nash and others (n 151).

Finally, despite some efforts in developing standards,[159] up until now there are no harmonised procedures to verify a child's age online.[160] Easy-to-use and adequate procedures are unreliable, as determined children can easily circumvent them by lying about their age or pretending to be their parents.[161] The simplest and most widely used, but also the easiest to circumvent, is the self-verification mechanism, where the user is asked for their birth date and access to a service or website is granted if they specify an appropriate age.[162] More advanced age verification methods are based on peer-review, that is, peers decide to grant access to a website or network based on users' profiles and on data collected elsewhere on the web or in the real world. In addition to self-verification, Facebook uses this method. These methods can also be circumvented easily by creating multiple profiles, and in addition, peer-based mechanisms can induce cyber-bulling. A new method of age verification is based on the automatic analysis of the semantics of users' profiles to deduce a user's age rage.[163] These mechanisms are typically difficult to circumvent, but they are complex to implement and not technologically mature, which make them prone to errors in a number of circumstances. Aside from this, it is also only possible to obtain the age range of a user, and not his or her exact age. Reliable alternatives to these methods include offline identity verification, identity verification using eID cards and using biometric data. The offline identity verification is typically implemented by directly contacting the parents or tutors of a minor to verify the age and eventually obtain parental consent to access a website or service. While reliable and effective, the method is also extremely complex. eID cards in contrast, are physical cards with a chip that contains data to perform age and identity verification online. These cards are typically obtained from trustworthy data sources, their use is simple for the user and relatively simple for the service providers to implement, while also being privacy friendly. However, the heterogeneous levels of implementation and the difficulty to enforce it as a standard have limited its popularity. Identity verification methods through biometric data exploit users' unique characteristics, such as fingerprints or iris patterns, to identify them. These mechanisms are reliable and very difficult to circumvent. However, the disclosure of such sensitive personal data raises ethical and privacy concerns. The Article 29 Working Party has called for caution in this respect on several occasions, emphasising that the use of biometrics may have a significant impact on the dignity, privacy and the right to data protection of young children and have potentially harmful effects (e.g. stigmatisation or discrimination due to their age or inability to enrol).[164] Moreover, there are

[159]The British Standards Institution is facilitating the development of Publicly Available Specification (PAS) 1296 Age Checking code of practice <http://trustelevate.com/age-checking-proof-of-concept-retail-sector/providers> accessed 1 March 2017.

[160]Article 29 Data Protection Working Party, 'Opinion 15/2011 on the definition of consent WP 187', 28.

[161]Jules Polonetsky, 'Online Age Verification for Our Children, A Report on the Tools and Resources Available for Safeguarding the First Generation of Digital Natives', The Future of Privacy Forum, 2009 <https://fpf.org/wp-content/uploads/2009/11/madrid-presentation-online-verification1.pdf> accessed 10 February 2017.

[162]boyd and others (n 126) 7 November 2011 (state that 'many parents now knowingly allow or assist their children in circumventing age restrictions on general–purpose sites through lying').

[163]Jules Polonetsky, 'Online Age Verification for Our Children, A Report on the Tools and Resources Available for Safeguarding the First Generation of Digital Natives', The Future of Privacy Forum, 2009 <https://fpf.org/wp-content/uploads/2009/11/madrid-presentation-online-verification1.pdf> accessed 10 February 2017.

[164]Article 29 Data Protection Working Party, 'Opinion 3/2012 on Developments in Biometric Technologies WP 193', 27 April 2012, 15.

Article 29 Data Protection Working Party, 'Opinion 3/2007 on the Proposal for a Regulation of the European Parliament and of the Council amending the Common Consular Instructions on Visas for Diplomatic Missions and Consular

additional concrete problems with the use of biometric data in case of minors. Due to the constantly changing bodily characteristics the biometric data of children become inaccurate and outdated much faster. Therefore, there are practical difficulties (inaccurate data could increase false acceptance or rejection rates and render the whole biometric application unreliable) and legal obstacles as inaccurate data processing contradict to the data quality requirements.[165] Moreover, biometric based methods are still complex to implement and do not allow an exact determination of a user's age.

Given the difficulties associated with finding age verification solutions that would be proportionate and reliable, more guidance and research is needed. The DPAs and the EDPB should take a position on the challenging and largely unresolved issue of age verification and provide guidance on the obligation to employ age verification for specific data collection practices, specific age verification methods and the level of acceptable reliability. As the Article 29 Working Party intends to adopt guidelines on consent in the GDPR in 2017,[166] the DPAs in UK,[167] Ireland[168] and France[169] have started gathering public views on possible solutions for age and consent verification.[170] In this context, UK ICO announced that it will start considering the area of children's privacy in order to form its own and European guidance on the issue[171] and issue guidance on how to identify a suitable lawful ground for processing personal data of children, and carry out age verification and parental authorisation.[172] In Germany, Bavarian DPA already issued a commentary on Article 8 and raised critical questions related to its unclear scope and interpretation.[173]

7. Moving forward and learning from the US experience

7.1. In the footsteps of COPPA … why is 13 not the best idea?

Although officially the EC has not directly explained or provided any other evidence to justify the choice, little doubt exist that the choice of 13 as the age threshold was

Posts in Relation to the Introduction of Biometrics, Including Provisions on the Organisation of the Reception and Processing of Visa Applications (COM(2006)269 final) WP134', 1 March 2007, 8.

[165]FIDIS, Biometrics in Identity Managements <http://www.fidis.net/resources/deliverables/hightechid/int-d37001/doc/19/> accessed 15 February 2017.

[166]European Commission (EC), 'Adoption of 2017 GDPR Action Plan' (Press release), 16 January 2017 <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083> accessed 15 March 2017.

[167]UK ICO, 'Consultation: GDPR Consent Guidance', March 2017 <https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf> accessed 10 April 2017.

[168]Data Protection Commissioner, 'Consultation on Consent, Profiling, Personal Data Breach Notifications and Certification', March 2017 <https://www.dataprotection.ie/docs/16-03-2017-GDPR-Call-for-consultation-on-consent-profiling-personal-data-breach-notifications-and-certification/1629.htm> accessed 10 April 2017.

[169]Commission Nationale de l'Informatique et des Libertés (CNIL), Consultation publique sur le règlement européen: Consentement, 23 February 2017 <https://www.cnil.fr/fr/consultation-reglement-europeen/consentement> accessed 1 April 2017.

[170]The CNIL public consultation on consent included the following questions:

> How can it be determined with certainty that the person concerned is a minor? How can the consent of the holder of parental responsibility be obtained when a minor is under 16 years old? How can specific consent for the collection of sensitive data be gained?

[171]UK ICO, 'Guidance: What to Expect and When' 2016 <https://ico.org.uk/for-organisations/data-protection-reform/guidance-what-to-expect-and-when/> accessed 13 March 2017.

[172]Kress and Nagel (n 100) 8.

[173]Bavarian Data Protection Authority, 'Information sheet for the implementation of the GDPR, No. 15', 20 January 2017 <https://www.lda.bayern.de/media/baylda_ds-gvo_15_childs_consent.pdf> accessed 3 April 2017.

influenced by COPPA. To a certain extent the EC itself has recognised the COPPA as being inspiratory. The GDPR's impact assessment published at the same time as the GDPR states: 'The specific rules on consent in the online environment for children below 13 years – for which parental authorisation is required – take inspiration for the age limit from the current US Children Online Data Protection Act of 1998'.[174] In addition, the EC admits that following the US legislative choice of the age of 13 would be beneficial for online business. The rules on consent, according to the EC's assessment, 'are not expected to impose undue and unrealistic burden upon providers of online services and other controllers'.[175] In fact, since the adoption of COPPA in 1998, the age limit of 13 has become a de facto standard for parental consent online, used not only by every US-based company, including the most popular social networking sites among children such as Facebook, Snapchat, Instagram, but also copied by a number of European service providers. The EC explicitly confirmed that it views the age of 13 as an existing standard during the debate at the Council of the EU.[176] Retaining the status quo would not have required so many changes or imposed new burdens on data controllers.

In addition, the US has exerted considerable influence on the GDPR text. Just before the end of the inter-service Consultation, which is one of the last steps in the adoption process of a new Commission legislative proposal, the US started a lobbying campaign against certain GDPR provisions proposed by the EC.[177] In an informal note submitted in December 2011 the US expressed its concerns in relation to diverging standards proposed by the EU GDPR and the obstacles they create vis-à-vis the interoperability between the EU and US privacy regimes.[178] The definition of a child as an individual under 18 in the GDPR was seen by the US as one of such obstacles for commercial interoperability. Defining children 'so broadly' according to the US is not advisable or feasible due to practical difficulties and can conflict with older children's rights to freedom of expression and access to information.[179]

The decision of the EC to propose the age of 13 as the threshold to allow children to consent to the processing of their personal data, as well as the final choice of the EU legislator to establish the age of 16 as the threshold, but allowing Member States to lower the limit to the age of 13 can be criticised.

First, the age threshold established by COPPA is of questionable use, as the US Congress adopted 13 as a consequence of a political compromise rather than as a well-reasoned or justified choice. Original drafts of this legislation defined children as individuals under the age of 18. When the legislation was introduced it referred to individuals under the age of

[174]Commission Staff Working Paper, Impact Assessment, SEC(2012) 72 final. <http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf>, 68.
[175]ibid 68.
[176]In the Council EC 'indicated that this [setting the age of consent at 13] was based on an assessment of existing standards, in particular in the US relevant legislation (COPPA)'. Proposal for a regulation of the European Parliament and of the 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), 16 December 2013 <http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2017831%202013%20INIT>, 77.
[177]EDRI, 'US lobbying against draft Data Protection Regulation', 22 December 2011 <https://edri.org/us-dpr/> accessed 1 January 2017.
[178]Informal note on Draft EU General Data Protection Regulation, December 2011 <https://edri.org/files/US_lobbying16012012_0000.pdf>; 'Informal Comment on the Draft General Data Protection Regulation and Draft Directive on Data Protection in Law Enforcement Investigations' <https://edri.org/files/12_2011_DPR_USlobby.pdf> accessed 1 March 2017.
[179]Informal note on Draft EU General Data Protection Regulation (n 178) 5.

16 and only in the final version was the age threshold lowered to 13.[180] This happened eventually to ensure the adoption of the law.[181] Equally proposals to raise the age limit for COPPA coverage were considered in 2010 when the rule was being updated.[182] For example, EPIC recommended Congress to raise the age requirement of COPPA to 18, mainly because 'the emergence of social networks and the powerful commercial forces that are seeing to extract personal data on all users of these services, but particularly children, raise new challenges that the original COPPA simply did not contemplate'.[183] The opponents argued that the extension of COPPA to teenagers would diminish privacy and anonymity by requiring age verification and data gathering of a large number of adults and raise profound free speech concerns.[184]

Second, the original intention[185] of COPPA was to protect children's personal information from commercial exploitation, primarily related to aggressive online marketing emerging in 1990s.[186] In fact, as claimed by EPIC, the choice of the age of 13 in COPPA predates many of the most intrusive and complex data collection practises online, such as the extensive behavioural tracking on social networking sites. Therefore, in light of COPPA's legislative history it is strange that none of the EU legislative bodies gathered fresh empirical evidence on the appropriate age threshold for parental consent in the GDPR. Instead of relying on COPPA as a legal transplant, the EU legislator could have questioned – using its own and up-to-date assessment – whether the age limit of 13; 1) can be translated into the completely different Web 2.0 of today and allows for the effective mitigation of risks associated with complex data gathering practises online predated by the original COPPA; 2) reflects the European culture and legal traditions of the EU Member States, as discussed above; and 3) is in line with the empirical research and evidence on children's Internet use.[187] In addition, the EU legislative bodies should have assessed whether its particular formulation of the parental consent requirement might have a negative impact on the child rights as a whole, which are strongly promoted by the EU itself. Assessments such as this would have allowed adherence to the UN CRC provisions and assessment of the impact of the GDPR by reference to all of the rights within the UN CRC. Ex ante child impact assessment is one of the fundamental steps in the EU child rights mainstreaming model. The lack of empirical evidence and failure to consult with

[180]Hoofnagle (n 109).
[181]EPIC, Testimony of Marc Rotenberg before the Senate Commerce Committee, 28 April 2010 <https://epic.org/privacy/kids/EPIC_COPPA_Testimony_042910.pdf> accessed 4 March 2017.
[182]ibid.
[183]ibid 9.
[184]Berin Michael Szoka and Adam D Thierer, 'COPPA 2.0: The New Battle Over Privacy, Age Verification, Online Safety & Free Speech' Progress & Freedom Foundation Progress on Point Paper No. 16.11, May 21, 2009; Comments to the FTC from the Center for Democracy & Technology ('Cdt'), The Progress & Freedom Foundation & Electronic Frontier Foundation ('EFF') <https://www.eff.org/files/coppacomments.pdf> accessed 15 February 2017.
[185]There is scholarly debate on the motivation behind COPPA. danah boyd and others argued that COPPA was motivated by privacy (see danah boyd, Urs Gasser and John Palfrey, 'How the COPPA, as Implemented, Is Misinterpreted by the Public: A Research Perspective', Statement to the United States Senate, April 29 2010 <http://cyber.harvard.edu/sites/cyber.harvard.edu/files/COPPA_Hearing_Statement_boyd_Gasser_Palfrey_4-29-10.pdf>; Chris Hoofnagle argues that the motivation related to both privacy and security from online predators (Hoofnagle (n 109)).
[186]Kathryn C Montgomery and Jeff Chester, 'Data Protection for Youth in the Digital Age: Developing a Rights-Based Global Framework' (2015)1(4) European Data Protection Law Review 291.
[187]Cf. EU Kids Online Project Reports <http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20Online%20reports.aspx>, Global Kids Online research results <http://blogs.lse.ac.uk/gko/results/>. See also Amanda Third and others, 'Children''s Rights in the Digital Age: A Download from Children Around the World' (Young and Well Cooperative Research Centre, Melbourne, 2014).

experts and stakeholders, including children,[188] unsurprisingly resulted into a wave of harsh criticism from child rights experts that have accompanied the developments on Article 8 from its conception to adoption.

7.2. Overreliance on (parental) consent and the need to shift protection from parents to data controllers

Although the GDPR establishes parental consent as a medium to protect children online, consent to personal data processing is not a panacea tantamount to giving control to individuals over their personal data in complex networked environments. Consent can provide illusionary control[189] and the agreement to the processing of personal data in situations of imbalance of powers is not delivered freely.[190] A rich body of literature points to the characteristics of networked environments that predetermine power imbalances and limit individuals in asserting control over their personal data.[191] Neither parents nor children can take full responsibility and control of their personal data online, as their choices and data management possibilities are shaped by the design and functionalities of communication spaces.[192] These communication spaces are far from neutral and are created to advance business interests rather than to allow the user to exercise their autonomy and control over their data. Informed consent online is hardly possible due to complex and ubiquitous data collection practises that do not yield to comprehensible privacy policies for service users.[193] In this sense, consent is often a result of a limited understanding of data collection consequences, as users do not actually read long and intricate privacy notices. Privacy policies, for children in particular, are long, complex, difficult to find[194] and easily confusing in their discourse (valorising 'sharing' and 'control', despite the extensive collection of children's data).[195] Consent can hardly be considered freely given when refusal to consent leads to social exclusion[196] given that important online services have no real alternatives. Various scholars have emphasised the weaknesses of consent as a protection mechanism online.[197] Many others have demonstrated that strengthening consent will not lead to a

[188]Article 12 of the UN CRC; Committee on the Rights of the Child (CRC) The right of the child to be heard (General comment No. 12) (2009) CRC/C/GC/12.

[189]Laura Brandimarte and others, 'Misplaced Confidences: Privacy and the Control Paradox' (2012) 4(3) Social Psychological and Personality Science 340.

[190]See, for example, Article 29 Data Protection Working Party, 'Opinion 8/2001 on the Processing of Personal Data in the Employment Context WP 48', 13 September 2001.

[191]Julie E Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (Yale University Press, 2012). Mireille Hildebrandt, 'Profiling and the Rule of Law' (2008) 1(1) Identity in the Information Society 55.

[192]Alice E Marwick and danah boyd, 'Networked Privacy: How Teenagers Negotiate Context in Social Media' (2014) 16 New Media & Society 1051.

[193]Lokke Moerel and Corien Prins, 'Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things' (25 May 2016) <https://ssrn.com/abstract=2784123> accessed 1 March 2017.

[194]Jacquelyn Burkell, Valerie Steeves and Anca Micheti, 'Broken Doors: Strategies for Drafting Privacy Policies Kids Can Understand' (report), March 2007 <http://www.idtrail.org/content/view/684/42/> accessed 10 April 2017; Sara M Grimes, 'Persistent and emerging questions about the use of end-user licence agreements in children''s online games and virtual worlds' (2013) 46(3) *UBC Law Review* 681.

[195]Valerie Steeves, 'Terra Cognita: Surveillance of Young Peoples' Favourite Websites' in Emmeline Taylor Tonya Rooney (eds) *Surveillance Futures: Social and Ethical Implications of New Technologies for Children and Young People* (Routledge, 2017).

[196]Ruth Furlong and Facer Keri, Beyond the Myth of the 'Cyberkid': Young People at the Margins of the Information Revolution (2001) 4(4) Journal of Youth Studies 451.

[197]Alessandro Mantelero, 'The Future of Consumer Data Protection in the E.U. Rethinking the 'Notice and Consent' Paradigm in the New Era of Predictive Analytics' (2014) 30 Computer Law & Security Report, 643. Bart W Schermer, Bart

greater individual control for individuals over personal data[198] and that consent cannot always be considered a legitimate ground for data processing.[199]

Yet, the GDPR is based on the premise that children can be protected through informed parental consent. As noted by Savirimuthu, 'since notice and consent are effectively meaningless, children are left with the predicament of making complex and undesirable trade-offs, resorting to social stenography techniques or accepting that the costs of obscurity is exclusion from participation in communities'.[200]

Not only consent in general but also parental consent in particular suffers from significant limitations both in terms of adequate protection and impact on children's rights. As regards adequate protection, there are many potential reasons why parental consent does not necessarily mean an increased protection of personal data for children. The GDPR requires consent to be sought from parents for all types of information society services in different sectors. An overload of consent requests may result in 'consent fatigue' among parents, when a constant consenting process becomes a disturbing irritation rather than a serious choice and can make the entire parental consent provision illusionary. The effectiveness of parental consent verification is still questionable, as due to the ambivalent and soft wording of the Article 8 in the GDPR, age verification depends on available technology and efforts of the industry that are considered 'reasonable'.[201]

In addition, the restriction of access to online services through parental consent, as formulated in the GDPR, might also have a negative impact on children's rights and autonomy.

Given that the consent requirement in the GDPR is fully applicable to all children under the nationally chosen age or the default age of 16 for all data processing cases that take place on the basis of consent, except for the preventive or counselling services, children might be restricted in their right to freedom of expression on the Internet. The UN CRC affirms that children are entitled to freedom of expression 'which includes the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the

Custers and Simone Van der Hof S, 'The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection' (2014) 16(2) Ethics and Information Technology 171; Eleni Kosta, *Consent in European Data Protection Law* (Brill/Martinus Nijhoff Publishers, 2013), 395–396.

[198]Lokke Moerel and Corien Prins, 'Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things' (25 May 2016) <https://ssrn.com/abstract=2784123> accessed 1 March 2017; Bert-Jaap Koops, The trouble with European data protection law (2014) 4(4) International Data Privacy Law *250*. Brendan Van Alsenoy, Eleni Kosta and Jos Dumortier, Privacy notices versus informational self-determination: Minding the gap (2014) 28(2) International Review or Law, Computers & Technology 185.

[199]Jean-Marc Dinant and Yves Poullet, The Internet and Private Life in Europe: Risks and Aspirations in A T Kenyon and M Richardson (eds), *New Dimensions in Privacy Law: International and Comparative Perspectives* (CUP, 2006), 72. ('Nevertheless consent does not appear to us to be a sufficient basis for legitimacy. We think that, in certain cases, the legitimacy of processing that is even backed by a person's specific, informed and freely given consent may be called into question. There are three reasons that support this view. First, consent that has even been obtained by fair means cannot legitimise certain processing that are contrary to human dignity or to other key values that an individual cannot relinquish. Second, consumers must be protected against practices that involve their consent being solicited in exchange for economic advantages. Finally, the question of the protection of privacy is not just a private matter but brings social considerations into play and calls for the possibility of intervention and marginal supervision by the authorities'.)

[200]Joseph Savirimuthu, 'Networked Children, Commercial Profiling and the EU Data Protection Reform Agenda: In the Child''s Best Interests?' in I Iusmen and H Stalford H (eds) *The EU as a Children''s Rights Actor: Law, Policy and Structural Dimensions* (Columbia University Press, 2016), 234.

[201]It could be claimed that in certain cases consent verification might become obligatory under Article 35 of the GDPR when data controllers perform data protection impact assessments and determine the appropriate measures (e.g. consent verification mechanisms) to comply with the GDPR.

child's choice'. The consent requirement in the GDPR positions parents as arbiters in deciding what is both allowed and beneficial for their children, without formally allowing children to influence their decisions. As noted by the Belgian Privacy Protection Commission, 'parental consent should not be a mechanism permitting a parent to override the child's decision unless there is a serious risk that the child will not correctly appreciate the consequences of its decision or that its natural naivety will be exploited'.[202] Parents may not always be in a position to fully grasp the best interest of the child. There could be cases of disagreement between parents and children over the usefulness and risks in relation to social media, and emotional, moral-panic driven or simply unjustified consent request rejections from parents. Counterintuitively, parents may become potential invaders of their children's privacy. For example, by using the right of access to personal data on behalf of their children, parents could monitor their children's online activities.[203] Also, parental consent mechanisms may become parental control systems and restrict the online freedoms of children.[204] Finally, the GDPR does not sufficiently take into account the right of the child to be heard, a fundamental principle of the UN CRC, and guarantee that the right of the child to express their views freely in all matters affecting them is taken into account in accordance with the age and maturity of the child.

Given the weaknesses of consent in general and parental consent in particular, the GDPR places an excessive burden on parents and children to make informed decisions about their personal data processing in the complex technology and data-driven environment.

More realistic possibilities to affect digital data collection practises and respond to children's needs and expectations would seem to entail shifting the responsibility from parents to data controllers. Instead of asking parents to control children's data collection through consent, the law could forbid some undesirable data collection practises through restrictions on the activities of data controllers. This would be in line with the thinking developed in the US after almost two decades of the COPPA experience. Hoofnagle claims that the real value of COPPA is in its limitation on personal data collection, use and retention through obligations on data controllers instead of the focus on parental consent requirement.[205] Montgomery echoes this view and argues that some children's data collection practises, such as profiling, behavioural advertising, cross-platform tracking, geolocation targeting should not be allowed by COPPA even with parental permission.[206] Similarly, Thierer claims that aside from education and empowerment, targeted enforcement of unfair and deceptive practices should be a way forward rather than parental consent and age verification expansion.[207] Boyd et al. suggest 'that policy–makers shift away from privacy regulation models that are based on age or

[202]Opinion (Avis) no. 38/2002 on the protection of the privacy of minors on the internet <http://www.privacy.fgov.be> accessed 1 March 2017.
[203]Hoofnagle (n 109).
[204]Simone van der Hof, 'No Child''s Play – Online Data Protection for Children' in Simone van der Hof, Bibi van den Berg and Bart Schermer (eds), *Minding Minors Wandering the Web: Regulating Online Child Safety*. Information technology and law series (24) (Springer with TMC Asser Press, The Hague, 2014).
[205]Hoofnagle (n 109) 215. ('(t)he real privacy protection in COPPA comes from its non-consent-related provisions, such as limits on data collection, use and retention')
[206]Kathryn C Montgomery and Jeff Chester, 'Data Protection for Youth in the Digital Age: Developing a Rights-Based Global Framework' (2015) 1(4) European Data Protection Law Review 291.
[207]Adam D Thierer, 'Kids, Privacy, Free Speech & the Internet: Finding the Right Balance' (12 August 2011). <http://ssrn.com/abstract=1909261> accessed 13 February 2017.

other demographic categories and, instead, develop universal privacy protections for online users' and 'provide parents with recommendations about the appropriateness of various sites for children of different ages and the various risks that users may face'.[208]

The GDPR entails provisions that limit the processing of children's personal data. The use of the legitimate interest of the data controller as a ground for lawful children's data processing is restricted in the GDPR. When the data subject is a child, it is highly probable that the legitimate interest of the controller are overridden by the interests or rights and freedoms of the child. Nevertheless, the legitimate interest ground can still be used by the data controllers in relation to children's data, but the assessment should be documented and the interest balancing exercise in general is likely to favour children as data subjects.

Recital 38 of the GDPR generally emphasises that specific protection should be afforded to children against marketing or profiling. Recital 71 refers to automated decision making based on profiling and states that such a measure should not concern children. This alludes to the conclusion that the profiling of children is prohibited, but upon closer scrutiny of both above-mentioned recitals, it appears that only automated decisions producing legal effects or otherwise significantly affecting the child are entirely forbidden. Taking into account the overarching objective of the GDPR to provide children as data subjects enhanced protection and the specific intention of the Member States to protect children against profiling clearly seen in the Council debate (discussed above), it would have been desirable to explicitly exclude children from profiling. It has been widely acknowledged that behavioural advertising is 'outside the scope of a child's understanding and therefore exceed the boundaries of lawful processing'.[209] As illustrated by Mc Cullagh

> children (and indeed most adults) are unlikely to be aware that inferences can be made from their disclosures – for instance, that 'liking' curly fries on Facebook is indicative of high intelligence or that 'likes' can be used to predict race or sexual orientation with a high degree of accuracy – and that both disclosed and inferred information can be used to generate profiles and produce targeted adverts.[210]

Yet, the vagueness related to children and profiling imbedded in the GDPR can be explained by practical challenges. It is questionable how effectively an explicit prohibition to profile children could have been enforceable in practice. It is still difficult to reliably distinguish between adults and children online.[211] An obligation to identify children in order to completely remove them from all targeting may lead to excessive data collection of a large number of adults, and instead of protecting one's privacy and anonymity online, could diminish and erode both.

The above mentioned restrictions, if effectively implemented, could have provided an alternative to the parental consent requirement as a protection model. Such restrictions on the collection of children's data, coupled with the respect for the fair data processing and accountability principles, would be better suited to diminishing its commercial exploitation in complex marketing, tracking and targeting systems, than parental consent.

[208]boyd and others (n 126).
[209]Article 29 Data Protection Working Party, 'Opinion 02/2013 on apps on smart devices WP 202', 27 February 2013.
[210]Karen Mc Cullagh, 'The General Data Protection Regulation: A Partial Success for Children on Social Network Sites?', in Tobias Bräutigam and Samuli Miettinen (eds) *Data Protection, Privacy And European Regulation in the Digital Age* (Unigrafia, Helsinki, 2016).
[211]van der Hof (n 204).

7.3. Deciding on the (single) age threshold

The GDPR sets a single age limit of 16 after which all children can be deemed competent to consent to the processing of their personal data, unless a Member State's national laws set a lower age which cannot go below the age of 13. A number of problems and challenges can be identified that need to be addressed before the GDPR comes into force.

Given the many different sectors and data collection practises, the choice of fixing a single age limit for consent in all data processing activities online has serious flaws. In order to guarantee adequate protection for children as data subjects but not excessively limit their online behaviour and rights, the context and data collection purpose should be taken into account. Different information society services might carry significantly different risks to a child's online safety and privacy. One and the same child may need protection for one data processing purpose, and may be able to autonomously consent to another. This is well illustrated by the case law in Germany. The Higher Administrative Court of Lüneburg[212] in a case related to video surveillance considered that the consent of a child may in general be invalid, if the child had not yet reached at least the age of 14 years. However, in 2012, the Higher Regional Court of Hamm[213] decided that it cannot be presumed that children between the age of 15 and 18 years would always have the required capability to foresee the consequences of the respective data processing operations. This case related to the processing of personal data for a sweepstake. The imposition of a single legal age-limit may disproportionally restrict the rights and opportunities for the child, irrespective of a child's own levels of competence in a specific context. Therefore, it might be worth considering the adoption of different age limits for different data collection areas and practices in the 13–16 age span. This might prove to be complex for children and parents to understand, but could provide more flexibility and account for the complexity and potential negative impact on children caused by specific data collection practices.

There could be several ways of determining the specific consent age limits and respective data collection areas. The Member States could adopt their national laws as they have the possibility to depart from the Regulation default age of 16. Detailed age limits and the identification of more and less risky data collection areas or purposes is unlikely to be achievable in the national data protection framework or other specific laws. In addition, for the industry this would result in increased disparity and an even more patch worked picture in every national jurisdiction. Codes of conduct at the European level therefore would seem to be a more flexible and less burdensome way of creating standards that account for children's vulnerabilities in a specific activity or sector, instead of treating all children as a homogeneous group of data subjects. As mentioned below, the GDPR creates conditions for the adoption of more effective codes of conduct.

If the Member States chose to legislate and lower the age threshold to 13, the industry codes of conduct could still go beyond this age requirement and guarantee stringent protection in specific data collection scenarios. Increasing the age limit up to 16 in voluntary codes of conduct in specific areas is therefore an option which would be in line with the GDPR requirements and provide added value by offering more protection for children's personal data in specific sectors.

[212]Germany, Case No. 11 LC 114/13.
[213]Germany, Case No. I-4 U 85/12.

During the GDPR adoption process the European institutions provided no evidence based on which the proposed age threshold would be grounded. The choice of the most appropriate age limit between 13 and 16, be it in national law or in self-regulatory initiatives, should be based on extensive empirical research. Social and behavioural sciences should be the first areas in which legislators gather solid and profound scientific evidence to justify any given age limit.

Also, until now, no public consultation to incorporate the voice of children has taken place.[214] During the GDPR adoption process adult driven discourse marked by a very protectionist stance in relation to children as internet users dominated. However, highly paternalistic and restrictive views have problematic consequences for children as rights holders, as 'such a narrow lens positions children solely as vulnerable victims, neglecting their agency and rights to access, information, privacy and participation'.[215] Consultations with relevant stakeholders, not only governments, industry, civil society, educational actors, but also children and parents themselves, should take place before taking decisions that affect children's rights and interests. It is well established that the views of children themselves should be considered in policymaking and the preparation of national laws related to the use of children's personal data, as well as in their evaluation.[216] As noted by the Committee on the Rights of the Child, 'including children should not only be a momentary act, but the starting point for an intense exchange between children and adults on the development of policies, programmes and measures in all relevant contexts of children's lives'.[217]

7.4. Pursuing the idea of age verification through innovative technological solutions

The implementation of Article 8 of the GDPR provides an opportunity for the EU to explore the different challenges and opportunities in adopting innovative online methods of age verification. Lessons can be learnt from national efforts and failures in the EU Member States and in the US. In the EU, several national age verification schemes using personal ID numbers have been facing shortcomings in terms of adequate enforcement, disproportionate data collection, and usability. In Germany, an attempt to use an age verification system based on the identity card or passport number coupled with the postal code of the city of its issuance has been declared by the German Federal Supreme Court as an effective barrier to prevent minors from accessing online age-restricted content.[218] In Belgium, the kids-ID card has been used as an online identification and age verification tool.[219] Using an integrated PIN and a card reader, from the age of six, children can identify themselves on the Internet with their kids-ID card and access online child-friendly chat rooms. However, this age verification tool has been criticised as too intrusive and

[214]Joseph Savirimuthu, 'Networked Children, Commercial Profiling and the EU Data Protection Reform Agenda: In the Child''s Best Interests?' in I Iusmen and H Stalford H (eds) *The EU as a Children''s Rights Actor: Law, Policy and Structural Dimensions* (Columbia University Press, 2016).

[215]Sonia Livingstone, John Carr and Jasmina Byrne, 'One in Three: Internet Governance and Children's Rights' (2015) Global Commission on Internet Governance Paper Series No. 22.

[216]Committee on the Rights of the Child, 'The Right of the Child to Be Heard' (General Comment No. 12) (2009) CRC/C/GC/12.

[217]ibid 5.

[218]See BGH vom 18.9.2007 – I ZR 102/05 – ueber18.de – OLG Düsseldorf, Zeitschrift für Urheber- und Medienrecht 2008, pp. 511–516.

disproportionate due to the use of the National Registry identification number embedded in the eID card revealing the date of birth and the gender of the child when only the identification of an individual as a child would be sufficient.[220] Also, the system was abolished quickly due to the fact that no children were found in the child-friendly chat rooms.[221] A more successful effort has been the SaferChat application implemented by the STORK project.[222] With the aim to implement EU-wide interoperability of electronic identities, the SaferChat created a safe online platform allowing for children from different EU Member States to communicate in chat rooms, using their national eIDs for identification, authentication and authorisation. Yet, the SaferChat application has been tested only as a pilot and did not yet lead to its sustainability in the long term or a wider take-up throughout the EU. In the US, as mentioned above, COPPA relies on users' self-assertion of their age which, as a method, is as easy to use as it is to circumvent. Children may often not be genuine in registering, use personal data that may not belong to them, and circumvent the age gating systems, for example by deleting cookies and restating a higher age. Lack of age verification if one of the main reasons for which COPPA has been widely claimed to be ineffective[223] and faces significant implementation and enforcement challenges. Notwithstanding this fact, the EC almost literally copied the COPPA parental consent requirement[224] in its proposal for the GDPR, ignoring the critics related to its ineffectiveness, without considering any alternatives of a more nuanced approach.

The EU should not blindly follow the US COPPA example, but pave the way in developing and adopting innovative and more effective age verification mechanisms. Given the challenges, there is a need to look for innovative age-verification mechanisms that are: (1) privacy-enhancing and respect data minimisation; (2) user-friendly and do not overburden the service providers; (3) do not limit children's opportunities provided by the Internet. The search for such solutions can be aligned with the EU's renewed interest and advancements in online authentication, attribute-based ecosystems and public e-ID schemes. The new Regulation 910/2014 on electronic identification (eIDAS Regulation) enables the adoption of secure eID throughout the EU and, accordingly, can facilitate age-related eligibility checks. In the context of the Audio Visual Media Services Directive, the EC asked content platform providers to explore the possibilities of leveraging secure eID, to conduct age-checks, in order to restrict children's access to harmful online content.[225] Consequently a multi-stakeholder group entitled the Alliance for Child Protec-

[219]The Belgian E-Id card has been designed to provide various functions: standard functions such as the proof of identity, a travelling document and a card for protection in emergency situations, in addition to acting as the online identification and age verification tool.

[220]Eva Lievens, 'Protecting Children in the New Media Environment: Rising to the Regulatory Challenge?' (2007) 24(4) Telematics and Informatics 315.

[221]Eva Lievens, *Protecting Children in the Digital Era* (Brill, 2010) 249, 408.

[222]STORK project, Pilot 2, Safer Chat – To promote safe use of the Internet by children and young people <https://www.eid-stork.eu/pilots/pilot2.htm> accessed 1 March 2017.

[223]Hoofnagle (n 109).

[224]Compare, for example, COPPA: 'An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology' with the EC Draft proposal: 'The controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology'.

[225]European Commission, Commission updates EU audiovisual rules and presents targeted approach to online platforms (Press release), Brussels, 25 May 2016 <http://europa.eu/rapid/press-release_IP-16-1873_en.htm>.

tion has been formed to examine how companies can use secure eID to improve the e-safety of children and develop codes of conduct.[226]

As age verification can range from verifying that an individual is above a certain age threshold, to knowing the exact age of a person and identifying an individual based on his age and other pieces of personal data (name, ID number, etc.), these various solutions have diverse implications to internet users' privacy. The EU should favour the least intrusive age verification method, such as relying on anonymous credentials and attributes through the creation of an appropriate legal framework, policies, technical architecture and standards. The use of attribute-based credentials in implementing Article 8 of the GDPR looks particularly promising, due to the advantages of minimal data disclosures and unlinkability.[227] In attribute-based schemes rather than verifying the full identity of an internet user, only a particular attribute, such as age, could be cross-checked in order to establish an internet user's eligibility to access an online service. Private technical architectures and standards are emerging on the market that are based on attributes and partial identity disclosure to prevent ineligible users from buying age-restricted goods, accessing age-restricted content and services.[228] These solutions that aim for pseudonymous and reliable age checks online could be considered when implementing Article 8 of the GDPR.

There is hardly a 'one-size fits all' solution for age verification that reflects the needs of different online service providers.[229] Different information society services with their particular data collection practises pose different degrees of risks to children as data subjects. As a result, methods of age verification that afford lower level of assurance might be adequate in lower risk online services, leaving high assurance options for high risk information society services.[230] This sliding scale approach is in line with the risk-based approach embodied into the GDPR, implying that the obligations of data controllers can be scalable according to the level of risk that their data processing poses to the rights and freedoms of the data subjects. The GDPR allows for the implementation of the sliding scale approach through data protection impact assessment and the adoption of safeguards, security measures and mechanisms to mitigate the risks, such as age verification of varying levels of assurance. High levels of assurance could be required for data processing involving profiling, marketing and other practises from which the GDPR considers that children merit specific enhanced protection.

Sliding scale age verification would less likely result in limiting online opportunities and benefits for children online, as the costs of obtaining age verification might lead to higher costs and lower revenues for data controllers, and consequently less valuable and interesting content for children. Proportionality is important for service providers, in the sense that 'the costs of age verification measures to be introduced must deliver enough benefit to

[226]European Commission, 'Commission to Broker a New Alliance to Better Protect Minors Online', 25 May 2016 <https://ec.europa.eu/digital-single-market/en/news/commission-broker-new-alliance-better-protect-minors-online> accessed 5 March 2017.

[227]On attribute-based credentials see Kai Rannenberg, Jan Camenisch and Ahmad Sabouri (eds), *Attribute-based Credentials for Trust: Identity in the Information Society* (Springer, 2015).

[228]See, for example, Trust Elevate's Age Check solution based on the attribute exchange ecosystem for pseudonymous age-related eligibility checks online and the development of PAS 1296 Age Checking code of practice <http://trustelevate.com/age-checking-proof-of-concept-retail-sector/> accessed 5 March 2017.

[229]Nash and others (n 151).

[230]ibid 3 (they claim 'the level of assurance (reliability) needed will vary across transactions: customer registration for an online gambling account will require both a wider range of information, and a higher level of assurance than would be needed to process the sale of a 15-rated DVD, for example').

the customer and the company to counter any additional costs (not just financial, but also in terms of time, convenience etc) imposed'.[231]

7.5. Consent verification driven by data controllers

When determining acceptable parental consent verification methods, the EU could learn some lessons from COPPA. In essence, the US embraces the co-regulation model, according to which if industry has a problem, the industry has the burden of solving it, and therefore it can propose responsible solutions approved by a regulator.[232] The FTC has a long history in working with the industry on methods of obtaining verifiable parental consent and deciding what methods are 'reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent'. The EU could equally establish a number of acceptable methods for gaining parental consent, at the same time encouraging interested parties to submit new verifiable parental consent methods for approval. It would actively incentivise the development of new age verification methods that are not only effective but also acceptable by the industry and suitable for specific sectors.

Codes of conduct could be one possible way to create standards for effective consent verification and specify Article 8 of the GDPR. Both the current DPD and the future GDPR encourages data controllers to adopt codes of conduct of industry associations that take account of the specific features of the various processing sectors. Codes of conduct are considered as 'market driven tools for application' of the GDPR provisions[233] and are attractive due the socio-technological expertise of the industry, innovation, reactive speed and reduced costs for the public bodies.[234] The GDPR provides additional incentives for data controllers to create or adhere to approved codes of conduct: adherence to a code of conduct may demonstrate compliance with the obligations of data controllers, provide the basis for international data transfers, be a positive factor in a Data Protection Impact Assessment and when fines are being imposed upon the adherent party. The GDPR explicitly refers to the protection of children and the manner in which parental consent should be obtained as one of the possible areas in which the GDPR's requirements could be specified (Article 40 GDPR). Thus, parental consent verification methods could be proposed by the industry through the codes of conduct.

Nevertheless, in order to ensure that self-regulation is accountable, efficient and able to deliver on its societal goals,[235] the EU should actively participate in the formulation of self-regulatory rules, and their effective monitoring and enforcement. Under the Directive 95/46/EC, the success of voluntary data protection codes has been very limited. The number of codes approved by the national DPAs vary significantly from one Member State to

[231]Nash and others (n 151).
[232]Ira Rubinstein, 'Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes' (2011) 6 A Journal of Law and Policy for the Information Society 356.
[233]Irina Vasiliu, 'Speech at the 7th Plenary Meeting of the Community of Practice for Better Self- and Co-Regulation. Synthesis of the Plenary', 24 June 2016 <http://ec.europa.eu/information_society/newsroom/image/document/2016-28/cop_7_-_synthesis_of_the_discussions_16585.pdf>
[234]Eva Lievens, 'Protecting Children in the New Media Environment: Rising to the Regulatory Challenge?' (2007) 24(4) Telematics and Informatics 315.
[235]European Commission, Principles for Better Self- and Co-Regulation <https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/CoP%20-%20Principles%20for%20better%20self-%20and%20co-regulation.pdf> accessed 2 February 2017.

another. At the European level, very few organisations representing specific sectors have tried, and only one of them has managed to draw up a code that was fully endorsed by the European DPAs.[236] The process of self-regulation took several years and was not necessarily shorter than a legislative procedure. Also, self-regulatory codes were limited in their ability to protect children as internet users, because of vague language, inadequate enforcement and monitoring mechanisms, and low market penetration.[237] In the area of online child safety, although little research is available on the actual impact of self-regulatory systems, the questionable efficacy of the major existing voluntary initiatives, such as the Safer Social Networking Principles for the EU, raise doubts as to their full implementation and compliance.[238] Stronger EU participation in the self-regulatory process, in particular rule formulation and enforcement, could help to achieve a better balance between the interests of children to exercise control over their personal data and the desire of businesses to valorise and profit from users' personal data. The GDPR, in contrast to the DPD, takes a step in that direction and requires: (a) DPAs to evaluate whether the code complies with the GDPR and, approve it, as well as register and publish the code; (b) an independent body, which has an appropriate level of expertise and is accredited by the competent supervisory authority, to monitor compliance with codes of conduct.

8. Conclusions

The growing importance of children's rights in EU policy making, empirical evidence vis-à-vis the risks for children and excessive and complex children's data collection practices online have driven the recognition in Europe that children's personal data deserves specific protection. The EU GDPR, which will be applicable from the 25th of May 2018, has established the requirement to obtain parental consent for the processing of the personal data of a child below the age of 16 years (unless national laws specifies a lower age threshold which cannot be lower than 13) when offering information society services (Article 8). Under the current Directive 95/46/EC, which has no specific rules on the consent of minors, the requirements related to the age and validity of consent have been diverging within the EU. Member States took three distinct approaches to regulate children's capacity to provide consent to their data processing, namely an objective bright-line, 'regulation by analogy', and a subjective capacity-based approach.

The analysis of the legislative history of Article 8 in the GDPR reveals the lack of well-reasoned justifications and evidence in terms of the substantive requirements adopted in the final version. With most of the GDPR debate being focused around articles with a direct economic impact on data controllers' activities and the Digital Single Market rather than the protection of vulnerable data subjects, Article 8 witnessed only sporadic renewals of interest during the debates in the EU institutions.

The EC almost literally copied the parental consent requirement from COPPA in its proposal for the GDPR, without taking into account the criticisms related to ineffective

[236]The only finalised code of conduct on the EU level is the 'European Codes of practice for the use of personal data in direct marketing' including an annex on online direct marketing by FEDMA <http://www.fedma.org/index.php?id=56> accessed 15 January 2017.

[237]Milda Macenaite, 'Protecting Children's Privacy Online: A Critical Look to Four European Self-regulatory Initiatives' (2016) 2 European Journal of Law and Technology.

[238]Jos De Haan and others, 'Self-Regulation' in Brian O'Neill, Elisabeth Staksrud and Sharon McLaughlin (eds) *Towards a Better Internet for Children. Policy Pillars, Player and Paradoxes* (Nordicom, 2013).

parental consent and age verification mechanisms or considering any alternatives of a more nuanced approach to child protection. Despite many valuable amendments being registered, the discussions at the European Parliament did not lead to major substantive changes either. The Council has only substantially deviated from the original GDPR proposal on the age of consent. It initially increased the age limit of consent to 16 years and in the last minute of negotiations took a flexible approach leaving the decision partially to the Member states. As a consequence, this left the EU without coherent and uniform age threshold in the European Digital Market and undermined the much-anticipated harmonisation effect of the GDPR. In summary, none of the EU institutions failed to employ an up-to-date means of assessment, question the age limit for consent, assess the impact on children's rights and the effectiveness of a particular formulation of the parental consent requirement, and to consider adopting a more nuanced version of parental consent.

Due to the failure to use well-reasoned justifications and evidence during the legislative process and the ongoing lack of guidelines, the GDPR parental consent requirement faces many practical challenges related to its interpretation and implementation. First, the requirement is applicable to information society services offered directly to a child. As information society services are normally provided for remuneration, this causes uncertainty as to the particular material scope of Article 8, especially its applicability to free services. Second, the requirement concerns online services offered directly to children, but it is complicated to draw the exact distinction between services to which the protection should apply. The extent to which the GDPR parental consent requirement will cover general-audience or mixed-audience services and sites remains unclear. The FTC solution of subjecting different services to a parental consent requirement through the 'totality of the circumstances test' and 'actual knowledge test' is useful, despite its flaws. Third, as the GDPR allows consent authorisation by the parents or the holders of parental responsibility over the child, it remains unclear if the reference to consent authorisation can be understood as allowing a joint consent and if the circle of holders of parental responsibility can include individuals other than parents and legal guardians. Fourth, to comply with the GDPR it suffices to make reasonable efforts to obtain verifiable parental consent rather than guarantee verified consent as a final outcome. It is not clear how much effort and proof in relation to obtaining consent can be requested from the controllers in order to sufficiently demonstrate compliance nor how reasonable efforts should be documented and proved. Fifth, specific parental consent mechanisms that can be used by data controllers to be compliant with the GDPR require further clarification and the guidance of the FTC on COPPA can be informative in specifying adequate and GDPR-compliant consent verification methods. Finally, the GDPR does not explicitly require the verification of a child's age, and thus more specification is needed on the relationship between consent and age verification, and the need for concrete proportionate and reliable age verification solutions.

Drawing on COPPA in the US, we identified pitfalls to be avoided and lessons to be learned when moving forward in the implementation of the EU parental consent requirement. Given the weaknesses of consent in general and parental consent in particular, the GDPR places an excessive burden on parents and children to make informed decisions about their personal data processing in the complex technology and data-driven environment. Instead of asking parents to control children's data collection through consent, restrictions on the most undesirable data processing practises in relation to children

should be enforced. Effective GDPR restrictions on children's data collection such as prohibition of profiling, marketing, the use of legitimate interest as a ground to process children's data, may provide an alternative to the parental consent requirement as a protection model. Purpose dependent restrictions on the collection on the collection of children's data would be better suited to diminishing its commercial exploitation in complex marketing, tracking and targeting systems, than parental consent.

The implementation of Article 8 of the GDPR provides an opportunity for the EU to address the different challenges and opportunities in adopting innovative online methods of age verification. Instead, of purely relying on the internet users' self-assertion of their age, as provided in the COPPA regime in the US, the EU should explore innovative, effective and privacy-friendly age verification mechanisms, aligning them with the advancements in online authentication, attribute-based ecosystems and public e-ID schemes. The use of attribute-based credentials in implementing Article 8 of the GDPR looks particularly promising, allowing for pseudonymous and reliable age checks online. In line with the risk-based approach embodied into the GDPR, methods of age verification that afford lower levels of assurance might be adequate in online services posing lower risks to the rights and freedoms of children, leaving high assurance options for high risk information society services, such as services involving profiling, marketing and other practises from which the GDPR considers that children merit specific enhanced protection.

When determining acceptable parental consent verification methods, the EU could follow the US example and encourage industry to propose effective, acceptable (from an industry perspective) and sector-tailored solutions for approval. Codes of conduct could be one possible way to create standards for effective consent verification and the further specification of Article 8 of the GDPR. Nevertheless, in order to ensure that self-regulation is accountable, efficient and able to deliver on its societal goals, the EU should actively participate in the formulation of self-regulatory rules, and their effective monitoring and enforcement.

As regards the age threshold for consent, it might be worth adopting different age limits for different data collection areas and practises in the 13–16 year age span. Specific consent age limits could be determined in national laws as Member States can depart from the GDPR default age of 16 or in codes of conduct at the European level. The latter could help to create standards that account for children's vulnerabilities in a specific activity or sector. If the Member States chose to lower the age threshold to 13, the industry codes of conduct could still go beyond this age requirement and guarantee stringent protection in specific data collection scenarios offering more protection for children's personal data depending on the context. In any case, the choice of the most appropriate age limit between 13 and 16, be it in national law or in self-regulatory initiatives, should be based on extensive empirical evidence and consultations with children.

Acknowledgements

The authors would like to thank Eva Lievens, Chris Hoofnagle, Daniel Cooper, and Damian Clifford for their insightful comments and suggestions. Any errors or omissions remain the responsibility of the authors.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

Eleni Kosta's contribution for this paper was made possible by a VENI personal research grant from the Netherlands Organisation for Scientific Research (NWO), project number 451-14-018.