Better Internet for Kids

The General Data Protection Regulation and children's rights:

questions and answers for legislators, DPAs, industry, education, stakeholders and civil society

Roundtable Report

23 June 2017

Brussels, Belgium

Contents

Executive Summary

"Feel free to answer questions with more questions."
– Patrick Geary (UNICEF)

From May 2018, the General Data Protection Regulation (GDPR) will take effect in the EU. The GDPR aims to strengthen, simplify and harmonise data protection regimes across Europe, giving individuals control over how their data are processed. It also explicitly acknowledges that children merit specific protection. Yet, from a children's rights perspective, article 8 GDPR – which contains requirements regarding parental consent for the processing of personal data of children under 16 (or 15, 14 or 13, if Member States so legislate) – has sparked a great deal of controversy and confusion. In addition, provisions regarding profiling and their application to children are the subject of diverging views.

Against this background, European Schoolnet, Ghent University and KU Leuven organised a Roundtable on the GDPR and children's rights on 23 June 2017 in Brussels, Belgium, bringing together a diverse group of around 100 legislators, data protection authorities (DPAs), industry, education stakeholders and civil society organisations to gather additional insight and develop a better understanding of different perspectives and possible implementation challenges.

This **Executive Summary** provides a succinct overview – session by session – of the main points raised during the Roundtable, while listing a number of questions which need further attention. It also explores how to more effectively involve children's rights organisations, parents' rights organisations, academia, industry, national DPAs, legislators and the education sector in the GDPR implementation process.

More specifically:

In ***Session 1: The GDPR: history, rationale and future guidance***, a brief overview was given of the challenging process of establishing the GDPR. The GDPR aims at restoring trust by putting EU citizens back in control of their data. It also includes a number of new elements for the protection for children, such as:

- Recital 58 GDPR which provides that, given that children merit specific protection, data controllers need to provide transparent privacy notices (i.e. information on any processing of their personal data) in clear and accessible language, so that the child can easily understand why and how his or her data is processed.
- Article 8 GDPR on parental consent and the age limit for children's consent. An important question in this regard is which age limit companies need to take into account when cross-border services are being provided? This question of private international law is being discussed in a group of experts of the Member States and several potential attachment criteria are on the discussion table (e.g. criterion of establishment, criterion of residence, etc.)

Other relevant changes introduced by the GDPR include the introduction of a data breach notification obligation for data controllers, a clearly spelled out right to be forgotten as well as a right to data portability for the data subject, a risk-based approach which makes obligations

dependent on the level or risks attached to data processing practices, a shift from ex ante to ex post enforcement and stronger sanction powers and independence for DPAs.

Apart from the opportunities it presents, the GDPR also raises a number of important challenges, such as:

- Difficulties concerning the implementation of the verifiable parental consent requirement.
- Difficulties for small NGOs and schools – which sometimes collect very sensitive data – to deal with GDPR requirements.
- Questions about the specific guidance that will be provided by DPAs in relation to the processing of children's data and children's rights – this is important given the major role DPAs will play in the implementation and enforcement of the GDPR.

In ***Session 2: Identification of children's rights issues in the implementation of the GDPR***, it was reiterated that the GDPR provides many opportunities to protect children, empower them and let them participate in all kinds of processes relating to them. However, the extent to which these opportunities can be achieved depends on how the provisions are implemented in practice.

The GDPR offers a few provisions that refer to children, either explicitly (e.g. articles 8, 12, 40 GDPR) or implicitly (by referring to the mechanism of article 8 GDPR, e.g. article 17 GDPR). Despite the fact that some important provisions do not mention children, they are nevertheless considered particularly relevant for children (e.g. article 25, 35 GDPR). Yet, there are many questions and issues that need clarification, for instance:

- Who is actually considered 'a child' under the GDPR?
- Consent is the most important ground for legitimising data processing activities. Article 8 GDPR is applicable to *information society services* (meaning almost any online service) being offered *directly to the child*. Neither of the notions are clarified at the moment.
- The parental consent requirement in article 8 GDPR also raises many practical questions regarding its implementation.
- Article 8 GDPR is a 'protection provision' but children's participation rights should also be taken into account.
- Aside from consent, there are also other legitimation grounds, such as the legitimate interests of the data controller. Article 6(1)(f) GDPR provides for a strict balancing test stating that processing is lawful when it is necessary for the purposes of the legitimate interests of the data controller, except where such interests are overridden by the interests or fundamental rights of the data subject, in particular where the data subject is a child. What does this imply in practice?
- Article 12 GDPR requires the provision of information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. How will this be implemented in practice?
- Other questions were raised about possible GDPR implications for the protection and provision of children's rights, for instance in relation to the right to erasure, profiling, privacy by design and by default, and data protection impact assessments (DPIAs).

In ***Session 3: Do children understand the commercial nature of the internet?*** a number of GDPR assumptions on what children can actually understand and at what age they can give an informed consent where questioned. Why was 13, 14, 15 or 16 chosen in particular and what basis will be considered by Member States when lowering the age threshold? In order to come up with measures to protect children's privacy, we need to know how children understand privacy in the digital environment. Unfortunately, there is very little evidence available on how children understand consent and when they are able to give it. It is crucial to understand how children's knowledge develops gradually and that this development is different for everyone. Meanwhile, well implemented legible terms and conditions would be an important step forward.

At the same time, the internet also provides enormous possibilities and benefits for children, including *inter alia* participation in civic activities, creative activities, networking, and education. Access to the internet is a matter of children's rights. If children are cut off from the internet, there might be costs in terms of potential benefits. Parents that are ignorant, busy or not present may deprive their children of opportunities. Is there any way to balance the risks and opportunities children are faced with?

In ***Session 4: Experiences from the United States and COPPA***, it was pointed out that, in the digital world, organisations engage in actions that are not always fair to children and consumers. Commercial practices now underpin a global industry and there is a need for international and global strategies on the protection of children as consumers. Digital media culture is very important to young people, it is fundamental in their lives and they should not be denied access to it. But how do we balance their rights to participate in this culture with fair privacy practices?

Twenty years ago, in the mid-nineties, an overall privacy policy in the US was lacking. This is the context in which a campaign for children's privacy rights was started and resulted in the adoption of COPPA (Children's Online Privacy Protection Act). The goals included education of the public, parents, policy makers and other stakeholders about the emerging commercial practices targeting children on the internet and staging an early intervention while the children's digital marketplace was in its formative stages. Key provisions of COPPA include limitations to the collection of personally identifiable information from children, mandating user-friendly and clear privacy policies, and requiring verifiable parental permission prior to the collection of data, thus providing an opt-in model for the processing of data of children under the age of 13. COPPA took effect in 2000 and its rules were revised in 2012 providing safeguards for mobile, geolocation, gaming and social media activities, expanding definitions of personally identifiable information also to photos and other online content, introducing restrictions on behavioural advertising, the use of 'cookies', and other persistent identifiers.

From a GDPR perspective, further reflection is needed on the (in)appropriateness of parental permission for children and teens, the need for safeguards that address adolescent developmental vulnerabilities, contemporary data collection and marketing practices, privacy by default, how to leverage stronger EU policies to establish global standards, how to educate DPAs and other critical stakeholders, and how to create coherent policy frameworks for dealing with the integration of data protection and marketing (including other EU and US

laws that might apply) and ensuring ongoing coordination among policy makers, researchers, and advocacy groups in the US and the EU.

In ***Session 5: Challenges for DPAs, industry, parents and children***, panellists addressed the fact that – while its goal was to harmonise and simplify data protection – the GDPR regulation is very complex and remains vague on many new concepts.

DPAs are likely to rely on the interpretation by the Article 29 Working Party as it would otherwise undermine the harmonising efforts of the EU legislator. Industry needs more guidance in interpreting and applying the text especially with regard to the requirements of accountability and self-assessment. One of the questions that should be addressed is what happens to legal certainty if there are not only different ages among different Member States, but also changing ages with changing governments? In addition, there are other legal instruments that create (further) uncertainty (e.g. the proposed e-Privacy Regulation, initiatives in the area of net neutrality, etc.), and it may be costly for start-ups to ensure compliance with these different frameworks. Consumers, from their side, need more legal certainty from industry, at least regarding the terms and conditions of companies.

It was also noted that the GDPR places the responsibility on parents on making informed decisions regarding their children's data. However, parents are often careless with their children's data themselves, do not necessarily want to be gatekeepers and are perhaps not willing to restrict their children's access to services. Parents expect that good standards, that will protect their children, are adopted and implemented.

Furthermore, a number of issues and questions were raised on, among others:

- The role of NGOs at national and EU level in relation to the enforcement and implementation of the Regulation;
- Self-assessment and verification mechanisms;
- The requirement for companies to prove that they have adopted reasonable measures to verify a child's age;
- The possibility of privacy dashboards and changing consent, as well as the lack of alternatives to the consent requirement.

From ***Session 6: Article 8, parental consent and codes of conduct***, a whole range of additional questions emerged. Most notably, it seems unclear what constitutes an 'information society service' 'directly offered to a child' in the context of article 8. Also, does the second element of this notion mean that article 8 GDPR only applies to services specifically targeting young children, for instance YouTube for Kids? Or does this refer to services that are used by children, although they are not specifically targeted to them (e.g. Facebook, eBay)?

Furthermore:

- An interesting point was made in relation to article 24 GDPR which requires every data controller to consider if there are any risks associated with that processing of personal data. It was argued that providers will not be able to implement this provision unless they know who their customers are exactly. In other words, the idea of knowing one's

customer must form part of the responsibility of every information society service provider.

- Different views were shared concerning the advertisement-based business models of online services. While there is no problem per se with advertising-funded services, there are problems associated with a certain type of business models, which are often incomprehensible for children as well as adults. There is a major difference between, for instance, Spotify giving recommendations based on user preferences and selling this information to third parties for marketing purposes.
- In terms of verification mechanisms, the DPAs of each Member State will have to provide guidelines on the solutions and approaches that are compliant with the GDPR. Simply because a good technological solution for age verification of children does not exist right now, it does not mean that it cannot be invented in the near future. At the same time, several participants raised doubts concerning the desirability of age verification as opposed to the idea of anonymity on the internet.

In ***Session 7a: Profiling, behavioural marketing and data protection impact assessments***, panellists were asked about the impact of profiling and behavioural marketing on individuals' rights.

According to one of the panellists, the question that needs to be asked is whether we want our children to grow up in a commercial surveillance world, with cross-device tracking and targeting, advertisements changing in real time, the rise of applications designed to bypass rational behaviour (i.e. neuro-marketing) and the establishment of huge data broker vehicles and marketing clouds.

Several panellists and Roundtable participants stressed that certain practices should be simply off limits for children under a certain age. This requires a granular discussion about children's developmental capacities. Additional safeguards are needed, for instance through specific sectorial regulation on privacy or an articulation of what the best practices relating to children should be. Notably, these safeguards should not limit children's participation and should be based on children's rights.

Participants also exchanged views on GDPR implications for behavioural advertising practices, possible alternatives to children's digital media experiences without personal data collecting, and the inclusion of children's views in privacy discussions.

In ***Session 7b: The implications for data protection and privacy education*** participants discussed possible future initiatives and measures, and their implementation in practice.

The need for trust in educators was emphasised, as well as trust in children themselves. It became apparent that many teachers are unaware of data protection implications. Meanwhile, the implementation of privacy-enhancing methods and digital literacy should not only focus on risks and the protection of children but also on empowering them by building their skills and understanding. Another challenge involves the difficulties of teaching children about the long-term consequences of sharing their data as they often seem not to be concerned about it. It was also agreed that parents – just like teachers – often lack the required skills in terms of privacy and data protection, which can make their children more vulnerable. Children, in spite of being somehow digital natives, do typically lack the knowledge and

maturity to fully understand the implications of certain behaviours and developments, so a dialogue between all relevant actors is critical.

Participants identified a number of solutions and action points, such as:

- Making data protection and privacy education an obligatory part of the curriculum, involving all teachers, staff and the school management in the topic, while integrating it across other subjects.
- A right to learn about data privacy/protection issues, and a system to support it should be implemented. Within this context, more attention should be given to corporate surveillance and unfair commercial practices.
- Resources, training and guidelines, including easy-to-use videos and online projects, should be developed to teach different stakeholders about e-safety, digital literacy, privacy and data protection.
- Involving industry is a must and schools cannot do it on their own. Thus, partnerships between schools, children's rights organisations, industry, parents' rights organisations and education networks such as European Schoolnet should be nurtured.

Full Report

"Feel free to answer questions with more questions."
– Patrick Geary (UNICEF)

From May 2018, the General Data Protection Regulation (GDPR) will take effect in the EU. The GDPR aims to strengthen, simplify and harmonise data protection regimes across Europe, giving individuals control over how their data are processed. It also explicitly acknowledges that children merit specific protection. Yet, from a children's rights perspective, article 8 GDPR – which contains requirements regarding parental consent for the processing of personal data of children under 16 (or 15, 14 or 13, if Member States so legislate) – has sparked a great deal of controversy and confusion. In addition, provisions regarding profiling and their application to children are the subject of diverging views.

Against this background, European Schoolnet, Ghent University and KU Leuven organised a GDPR Roundtable on children's rights on 23 June 2017 in Brussels, Belgium, bringing together a diverse group of around 100 legislators, data protection authorities (DPAs), industry, education stakeholders and civil society organisations to gather additional insight and develop a better understanding of different perspectives and possible implementation challenges.

This **Full Report** provides a detailed overview – session by session – of the main points raised during the Roundtable, while listing a number of questions which need further attention. It also explores how to more effectively involve children's rights organisations, parents' rights organisations, academia, industry, national DPAs, legislators and the education sector in the GDPR implementation process.

Session 1: The GDPR: history, rationale and future guidance

Karolina Mojzesowicz (Deputy Head of Unit, European Commission, DG Justice and Consumers, Unit C3, Data Protection)

Reasons for a new European framework on data protection

As an introduction, a brief overview was given of the challenging process of establishing the GDPR. A new legislative instrument was needed for several reasons: (1) Directive 95/46/EC (Data Protection Directive; DPD) does not fully address the enormous technological advancements and globalisation, (2) the fundamental right to data protection was constitutionalised through the Lisbon Treaty and (3) national legislative frameworks were fragmented. The GDPR addresses these challenges and allows businesses to use the opportunities new technologies may bring, while at the same time ensuring that it happens in accordance with society's views and wishes. In this regard, studies conducted by the European Commission (EC) showed a **trust deficit** among EU citizens in online services (e.g. online payment via credit cards). The GDPR aims at restoring this trust by putting individuals back in control of their data. Although there is a continuity of rights when comparing the '95 DPD and

the GDPR, there are certain amendments and updates, especially in relation to exercising the rights and an increased harmonisation (i.e. one set of rules for all Member States).

New elements of protection for children

An important element that is introduced by the GDPR is **recital 58 GDPR** which provides that, given that children merit specific protection, data controllers need to provide **transparent privacy** notices (i.e. information on any processing of their personal data) in clear and accessible language, so that the child can easily understand why and how its data is processed. This goes hand in hand with the clarified provision on **informed consent** as a ground for processing personal data. Valid consent under the GDPR requires a clear affirmative action (i.e. no pre-ticked boxes, no implied consent). Data controllers need to ensure that the person from whom they are obtaining the consent understands what he or she is consenting to, also when this person is a child. Moreover, it is a continuous process for the data controller, who needs to be able to prove this to the DPAs.

In **article 8 GDPR** on parental consent and the age limit for children's consent, the EC aimed for a higher level of protection (compared to the DPD) by analysing the situation around the world (e.g. US Children's Online Privacy Protection Act (COPPA)) and tried to introduce some of the solutions provided there (e.g. verifiable parental consent for minors under the age of 13). However, the European Parliament and Council did not agree on one age, as the issue of children's consent is very much linked to the civil law traditions at the national level, where different ages of consent are set. Therefore, the agreement and solution found was to provide room for manoeuvre, by offering Member States the possibility to derogate from the age of 16, to 15, 14 or 13.

An important question in this regard is **which age limit companies need to take into account** when **cross-border services** are being provided? This question of private international law is being discussed in a group of experts of the Member States and ***several potential attachment criteria*** are on the discussion table:

- ➔ ***Criterion of establishment***: A data controller is established in Member State X (age limit of 13 years) and offers its services in Member State Y (age limit of 14 years), then Member State Y could accept the age limit of the Member State where the controller is established. Germany and the Netherlands have indicated a preference for this criterion.
- ➔ However, if the establishment is made for the *sole purpose of circumventing* this rule, then the rules of the other Member State would apply: if a data controller is established in Member State X to circumvent the age limit of Member State Y but only targets its services to citizens of Member State Y, then the age limit determined by Member State Y would apply.
- ➔ ***Criterion of residence***: Some Member States want their laws to apply to the individuals residing in their territory. So, for children residing in Member State X that are targeted with services by a provider established in Member State Y, the age limit determined by Member State X applies.
- ➔ Possibly other criteria might be considered as well.

Other changes introduced by the GDPR

Other major changes include the introduction of a data breach notification obligation for data controllers and a clearly spelled out right to be forgotten as well as a right to data portability for the data subject. Furthermore, the GDPR follows a **risk-based approach**, as the set of obligations imposed on the data controller depends on the level of risks attached to his or her data processing practices. Accordingly, there is a scalability of obligations: the more a controller processes sensitive data or children's data, the more obligations this controller has. Moreover, according to the **accountability principle**, the data controller has to ensure that the data protection rules are complied with (i.e. self-assessment), from the beginning until the end of the processing activities.

Finally, the GDPR also marks a **shift from ex ante to ex post enforcement** by granting the DPAs stronger sanction powers and strengthening their independence. DPAs can issue fines that can go up to 2-4 per cent of a company's worldwide annual turnover, depending on the circumstances. The GDPR ensures a uniform interpretation and application of the rules throughout the EU by providing a consistency mechanism and the EU Data Protection Board, which can take binding decisions on interpretation disputes. Data controllers have less notification obligations and only have to conduct data protection impact assessments when there is a high risk. The Article 29 Working Party is currently developing **guidelines on consent, profiling, transparency and data breach notification and data protection impact assessments.** The EC is also in dialogue with different stakeholders to develop codes of conduct for data controllers.

Several participants brought up the **difficulties concerning the implementation of the verifiable parental consent requirement**. What if a child or parent provides a false age? The speaker stressed that it is up to the controller to prove that he/she did their utmost best, in accordance with the state of the art of the available technology, to ensure that valid consent is given. Another participant highlighted that it will be very difficult for small NGO's or schools, which sometimes process very sensitive information, to deal with these requirements.

Another participant mentioned that the last time the Article 29 Working Party looked into children's personal data was in 2010. It was stressed that DPAs are going to be the major players, yet they are not very well informed about the issues concerning the use of children's data. The speaker noted that these **issues will not be addressed in a specific guidance document** that relates only to the impact of the GDPR on children, but will be dealt with within the different guidelines that are currently being prepared (e.g. the guidance document on profiling could also contain a section on the profiling of children).

Questions raised:

- *Which age limit will companies need to take into account when cross-border services are being provided?*
- *Will Member States choose the criterion of establishment, the criterion of residence or other criteria for the provision of cross-border services?*
- *To what extent guidance will be provided by the Article 29 Working Party and DPAs in relation to the implementation of the GDPR regarding children?*
- *Regarding the implementation of the verifiable parental consent requirement, what measures will data controllers take if a child or parent provides a false age?*

- *What are the difficulties for small NGO's or schools, which sometimes process very sensitive information, when dealing with these requirements?*

Session 2: Identification of children's rights issues in the implementation of the GDPR

Prof. Simone van der Hof (Leiden University)
Prof. Eva Lievens (Ghent University)

The GDPR provides many opportunities to protect children, empower them and let them participate in all kinds of processes relating to them. However, the extent to which these opportunities can be achieved depends on how the provisions are implemented in practice. The GDPR offers a few provisions that refer to children, either explicitly (e.g. articles 8, 12, 40 GDPR) or implicitly (by referring to the mechanism of article 8 GDPR, e.g. article 17 GDPR). Despite the fact that some important provisions do not mention children, they are nevertheless considered particularly relevant for children (e.g. article 25, 35 GDPR). Yet, there are **many questions** and issues that need **clarification**.

Who is actually considered 'a child' under the GDPR? According to the UN Convention on the Rights of the Child (UNCRC), a child is a person under 18. The **definition** was initially included in one of the drafts of the GDPR but was removed in the final version of the regulation. Only article 8 GDPR mentions the age of the child specifically, in relation to the direct offer of information society services and parental consent. Does this mean that all other articles that have an impact on children refer to anyone under 18?

Another unclarity concerns the provision on **children's and parental consent** (article 8 GDPR). Consent is in many cases the preferred ground for legitimising data processing activities. Article 8 GDPR is applicable to *information society services* (meaning almost any online service) being offered *directly to the child*. Neither of the notions are clarified at the moment. Additionally, in situations where children cannot consent themselves, the consent must be *given* or *authorised* by the holder of parental responsibility over the child. The fact that both of these notions are mentioned seems to imply that they are different. Neither the meaning of both notions, nor the difference between them are clarified.

The **parental consent** requirement in article 8 GDPR also raises many practical questions regarding its **implementation**. For instance, how will companies verify that the person providing consent is actually the parent? Data controllers will have to make reasonable efforts to ensure compliance in accordance with the current technological state of the art (e.g. through self-regulation or certification). It is not clear what would constitute a 'reasonable effort'. Notably, some companies will be in a much better financial position to invest in the necessary measures than others. In terms of technical possibilities, the remaining questions cover the likelihood of the implementation measures leading to more processing of personal data and how companies will deal with children circumventing the parental consent requirement. After all, children do have a right to have private spaces to themselves on the internet without their

parents' interference. Clearly, article 8 GDPR is a 'protection provision' but children's participation rights should also be taken into account.

Aside from consent, there are also other legitimation grounds, such as the **legitimate interests of the data controller**. When this ground is relied upon, there will be a need for a balancing test in order to ensure equal protection of the different interests at stake. Article 6(1)(f) GDPR provides for a strict balancing test stating that processing is lawful when it is necessary for the purposes of the legitimate interests of the data controller, except where such interests are overridden by the interests or fundamental rights of the data subject, **in particular where the data subject is a child**. The phrasing "*in particular*" implies that the balancing test for the processing of the personal data of children is stricter. The question arises whether that is true and, if so, how much stricter? Again, the provision does not mention any specific age.

Article 12 GDPR requires the **provision of information** in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. Transparent information is extremely important as children will only be able to exercise their rights if they know what those rights are. How will this be implemented in practice? This should be done by means of text or visuals that actually mean something to children. The design of layered notices, or the use of co-creation methods where children participate in the process of drafting and testing innovative techniques, to ensure that the information is really transparent to them (and their parents, for that matter), should be considered. Uncertainty remains as to how the DPAs will enforce the provision on transparent information and check that the controllers comply with these provisions.

Article 17 GDPR provides for the **right to erasure** ('the right to be forgotten'). It puts more emphasis on what this right can mean for children. In cases where a child has given consent and later wants to remove the data, this article could be useful (see also recital 65 GDPR). However, it is unclear how it will be implemented in practice. And again, children will only be able to exercise this right if they are aware, not only of the right in itself, but also of which data is actually being processed. For some data this might be obvious, for instance for 'given data', for other types of data it might be more difficult to understand.

Recital 38 GDPR mentions profiling as one of the activities for which children merit specific protection. However, article 22 GDPR, regulating automated individual decision-making, including **profiling**, does not mention children. It does confer the right upon a data subject not to be subject to profiling, which produces a legal or a similarly significant effect. Recital 71 GDPR provides that 'such a measure' should not concern a child. Although it has been argued that this means that profiling of children is prohibited, a close reading of the article shows that this is only the case if a decision is made that has *a legal or similarly significant effect***.** Examples for adults of such decisions include an automatic refusal of an online credit application or e-recruiting practices without any human intervention. But what does that mean for a child exactly? Could it relate to the offer of education, criminal justice or youth care? Does article 22(2)(c) GDPR allow profiling of children after all if explicit consent is given? Can a child give an informed consent in this case? Will this depend on age?

The provisions on **privacy by design and by default** (article 25 GDPR) are particularly useful mechanisms for children but it remains to be seen how will they be integrated within current technologies. Could there be default settings in relation to certain privacy intrusive practices

that may vary according to age and evolving capacities? It would not seem unreasonable to expect that products aimed at children, such as connected toys, integrate important principles, such as data minimisation, in the design of the products. Perhaps data minimisation could, in any case, mean something different when personal data of children are concerned.

Article 35 GDPR concerns **data protection impact assessments (DPIAs)** and requires a prior assessment when a high risk to the rights of a data subject exists. The recitals on what may constitute a high risk do not mention children but they do mention profiling (recital 91 GDPR). In light of the specific protection of children and the accountability principle, it could be a good practice to carry out DPIAs every time personal data of children are being processed. Will other rights of the child, such as freedom of expression, be taken into account in such a DPIA? Inspiration to carry out children's rights oriented DPIAs could be drawn from the work that UNICEF has been doing in this area. The results of the DPIAs could also provide feedback on the implementation of new privacy by design and privacy by default mechanisms.

The speakers concluded that, aside from the many questions that are raised by the GDPR in relation to children, what is perhaps even more important are the issues and possible measures that are *not* explicitly mentioned in the text of the new regulation. For instance, how can or should specific protection for children between the age of consent (article 8 GDPR) and 18 be provided? Should there be additional safeguards, for instance with regard to privacy-invasive measures such as profiling and behavioural targeting? Notably, all questions that arise should be addressed **from a children's rights perspective.**

Questions raised:

- *Who is considered 'a child' under the GDPR?*
- *In terms of article 8 GDPR, what are information society services and what does 'offered directly to the child' mean?*
- *In terms of article 8 GDPR, what does 'given' and 'authorised' consent mean and what is the difference between these two notions?*
- *How will companies verify that the person providing consent is actually the parent?*
- *What will constitute a 'reasonable effort' made by data controllers when ensuring compliance?*
- *Will the implementation measures of article 8 GDPR lead to more processing of personal data?*
- *How will companies deal with children circumventing the parental consent requirement?*
- *Is the balancing test for the processing of the personal data of children in terms of article 6(1)(f) GDPR stricter and if so, how much stricter?*
- *In terms of article 12 GDPR, how will the provision of information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, be implemented in practice?*
- *How will the DPAs enforce the provision on transparent information and check that the controllers comply with these provisions?*
- *How will the right to erasure (article 17 GDPR) be implemented in practice?*
- *What does a legal or similarly significant effect of automated decision making (including profiling) mean to a child? Does article 22(2)(c) GDPR allow profiling of children if explicit consent is given? Can a child give an informed consent in this case? Will this depend on age?*

- *How will privacy by design and privacy by default mechanisms (article 25 GDPR) be integrated within current technologies? Could there be default settings in relation to certain privacy intrusive practices that may vary according to age and evolving capacities? Could data minimisation mean something different when personal data of children are concerned?*
- *Will other rights of the child, such as freedom of expression, be taken into account when DPIAs are carried out?*
- *How can or should specific protection for children between the age of consent (article 8 GDPR) and 18 be provided? Should there be additional safeguards, for instance with regard to privacy-invasive measures such as profiling and behavioural targeting?*

Session 3: Do children understand the commercial nature of the internet?

Prof. Sonia Livingstone (LSE)

The GDPR intends to protect children's data but it makes crucial assumptions on what children can actually understand and at what age they can give an informed consent without explaining the grounds for such assumptions. Why was 13, 14, 15 or 16 chosen in particular and what basis will be considered by Member States when lowering the age threshold? Unlike when COPPA (Children's Online Privacy Protection Act) was considered in the United States (US), public debates on the possible age threshold were never held in Europe despite the fact that positive rights of children as internet users might be drastically and unequally restricted.

In order to come up with measures to protect children's privacy, we need to know how children understand privacy in the digital environment. Unfortunately, there is **very little evidence available on how children understand consent and when they are able to give it**. Most research has been conducted on consent in the context of medical procedures and research itself, but in these cases consent is very individual. Some research on how children understand privacy in their relationships has been conducted and revealed that children tend to make decisions in the context of a particular relationship (cf. the notion of 'contextual integrity' by Helen Nissenbaum) and social norms. The psychological context of children's decision making is very multidimensional and complex. Children are persuaded by different pressures in different contexts. Decision-making in a commercial environment can be very specific, thus, more research is needed and it should actually have been conducted *before* the GDPR was passed.

It is crucial to understand how children's knowledge develops gradually and that this development is different for everyone. According to research conducted by Ofcom (the communications regulator in the UK), children's background has a significant effect on their understanding. The same research has shown that a 15-year-old in a poor home knows about the same as an 11-year-old in a rich household. How does the GDPR relate to such findings? In terms of parents, the more responsibility they take and the more actively they parent, the higher the chance of their children understanding commercial practices. Further, if children engage in a high number of activities on the internet they appear to know more about commercial

practices. Thus, **restricting access to certain services to under 16s would also lead to reduced knowledge**.

Literacy and legibility is extremely important in this context. What we understand depends on what is presented to us. In other words, competence depends on what information people are presented with. Media literacy abilities develop between 13 and 16 years but *there is no magic switch*, thus we need to question why 13 or 16 years is being used in the GDPR as it depends on capacities and context. Unfortunately, the big companies are not yet presenting legible information to their users. **Well implemented legible terms and conditions** would be an important step forwards by data controllers. However, it should be stressed how difficult the rewriting of terms and conditions can be. In addition, special attention should also be given to teenagers and their protection. More research is needed into how commercially interesting they are to companies and how they should be protected.

The internet provides enormous possibilities and benefits for children, including *inter alia* participation in civic activities, creative activities, networking, and education. Access to the internet is a matter of children's rights. If children are cut off from the internet, there might be costs in terms of potential benefits. Parents that are ignorant, busy or not present may deprive their children of opportunities. Is there any way to better balance the risks and opportunities children are faced with?

Questions raised:

- *In terms of article 8 GDPR, why was 13, 14, 15 or 16 chosen in particular and what basis will be considered by Member States when deciding whether or not to lower the age threshold?*
- *How do children understand commercial practices in the digital environment?*
- *How does the GDPR take into account differences in children's social background, context, capabilities and development?*
- *What about the protection of adolescents? How commercially interesting are they to companies and how should they be protected?*
- *Is there any way to better balance the risks and opportunities children are faced with on the internet?*

Session 4: Experiences from the United States and COPPA

Prof. Kathryn Montgomery (American University)

In the digital world, organisations engage in actions that are not always fair to children and consumers. The way in which connected toys are designed is just one example. The interactive Cayla doll, for instance, talks to children about her favourite Disney movies. Commercial practices now underpin a global industry and there is a need for international and global strategies on the protection of children as consumers. Notably, digital media culture is very important to young people, it is fundamental in their lives and they should not be denied access to it. But **how do we balance their rights to participate in this culture with fair privacy practices**?

Twenty years ago, in the mid-nineties, an overall privacy policy in the US was lacking. The public policy debate was dominated by safety, cyber-porn and other concerns, and there was very little public awareness of emerging business models and practices. Gradually, one-to-one marketing and advertising strategies appeared that started to engage individually with every child. Early advertising research revealed that when a child was online, he or she went into a 'flow stage' and took in all the information presented to them unconsciously. As a consequence, advertisers started developing personal relationships between children and products.

This is the context in which a campaign for children's privacy rights was started and resulted in the adoption of COPPA (Children's Online Privacy Protection Act). The goals included education of the public, parents, policy makers, and other stakeholders about the emerging commercial practices targeting children on the internet and staging an early intervention while the children's digital marketplace was in its formative stages. Trying to limit data collection and promote fair marketing practices for children, the campaign was, in fact, helped by the European Union as the DPD was adopted in 1995 and came into force in 1998. Notably, COPPA was passed right on the day when the Directive became applicable in the EU in October 1998. Key provisions of COPPA include limitations to the collection of personally identifiable information from children, mandating user-friendly and clear privacy policies, and requiring verifiable parental permission prior to the collection of data, thus providing an opt-in model for the processing of data of children under the age of 13. COPPA took effect in 2000 and its rules were revised in 2012 providing safeguards for mobile, geolocation, gaming and social media activities, expanding definitions of personally identifiable information also to photos and other online content, introducing restrictions on behavioural advertising, the use of 'cookies' and other persistent identifiers.

At the moment, we live in a world where a lot of money is being generated by new digital players, we live multi-screen ubiquitous lives, data collection has reached its highest levels and data controllers know who we are, what we think and even how we feel. This environment creates significant concerns such as big data practices (profiling, 'digital dossiers', discrimination), erosion of privacy, traditional 'user-control' models being increasingly challenged, commercialisation affecting the health and wellbeing of young people, creation of unfair marketing techniques, the rise of equity issues such as the requirement to 'pay for privacy' and quality non-commercial content being hidden behind a pay wall which may impact low-income children. Thus, specific suggestions for discussion include parental permission which is appropriate for young children but not for teens, the need for safeguards that address adolescents' developmental vulnerabilities, contemporary data collection and marketing practices, privacy by default, leveraging stronger EU policies to establish global standards, educating DPAs and other critical stakeholders, creating coherent policy frameworks for dealing with integration of data protection and marketing (including other EU and US laws that might apply) and ensuring ongoing coordination among policy makers, researchers, and advocacy groups in the US and the EU.

Questions raised:

- *How do we balance young people's rights to participate in today's digital environment with fair privacy practices?*

- *How can safeguards for adolescents' developmental vulnerabilities be implemented?*
- *How do we educate DPAs and other critical stakeholders?*
- *How do we ensure ongoing coordination among policy makers, researchers, and advocacy groups in the US and the EU?*

Session 5: Challenges for DPAs, industry, parents and children

Caroline De Geest (Belgian Privacy Commission), Andrea Parola (ICT Coalition), David Martin (BEUC), Vicki Shotbolt (Parent Zone)

Moderator: Prof. Peggy Valcke (KU Leuven)

Each of the panellists was invited to give an **elevator pitch** of their first impressions of the challenges for different stakeholders.

First, it was discussed that, while the goal of the GDPR was to harmonise and simplify data protection, the regulation is very complex and remains vague on many new concepts. In this regard, **DPAs** rely on the interpretation by the Article 29 Working Party as it would otherwise undermine the harmonising efforts of the EU legislator. Considering the complexity and vagueness of the text, **industry** needs more guidance in interpreting and applying the text especially with regard to the requirements of accountability and self-assessment. One of the questions that should be addressed is what happens to legal certainty if there are not only different ages among different Member States, but also changing ages with changing governments? In addition, there are other legal instruments that create (further) uncertainty (e.g. the proposed e-Privacy Regulation, initiatives in the area of net neutrality, etc.), and it may be costly for start-ups to ensure compliance with these different frameworks. **Consumers**, from their side, need more legal certainty from industry, at least regarding the terms and conditions of companies. BEUC (the European Consumer Organisation or *Bureau Européen des Unions de Consommateurs*) expressed its concern about the practices that are going on, such as emotional harvesting online, and stressed that it is crucial to keep up with these business initiatives. Finally, it was noted that the GDPR places the responsibility on **parents** on making informed decisions regarding their children's data. However, parents are often careless with their children's data themselves, do not necessarily want to be gatekeepers and are perhaps not willing to restrict their children's access to services. Parents expect that good standards, that will protect their children, are adopted and implemented.

Questions were raised on the **role of NGOs** at national and EU level in relation to the enforcement and implementation of the Regulation. Specifically, could litigation be initiated by NGOs in order to hold industry accountable? Notably, BEUC plays an important role in this regard as their goal is to ensure that novel and problematic practices are researched, and that businesses are kept in check. Moreover, BEUC could represent data subjects in court.

Issues concerning self-assessment and verification mechanisms were also brought up. In particular, how could children be better protected and **how can data protection impact**

assessments take children's interests into account? It was suggested that industry should make a stronger effort to inform consumers and communicate with parents who are actually enabling their children to connect. On the other hand, it was stressed that these issues go beyond creating transparency and providing information to parents and children. Some practices of commercial entities should simply not be taking place in the first place as they are unfair to consumers. More money should be spent on promoting safety and helping smaller companies to comply with the rules.

Moreover, questions were raised regarding the **requirement for companies to prove that they have adopted reasonable measures to verify a child's age.** Are companies collaborating on the creation of feasible methods and what is the state of the art of the current technological possibilities? Also, are consumer organisations cooperating with companies on the technological issues? It appears that certain companies are already trying to find technological solutions. Crucially, the key requirement for companies is the requirement of '*reasonable efforts*'. 'Reasonable efforts' could perhaps mean something different for big companies and SMEs. In this regard, industry calls for legal certainty and clear rules for companies. It was also highlighted that the implementation of the verification requirement imposed on companies could violate the principle of data minimisation. Companies should only require the information that they really need for verification and the provision of the service. In this regard, requiring an ID card might go too far, thus, a child should be able to prove his or her age using other means.

The possibility of **privacy dashboards and changing consent** was also mentioned. In particular, service providers should be able to give feedback to consumers on what data they are using and, on the basis of this, consumers should be able to change their consent if they wish to do so. Panellists stressed that it should be as easy to withdraw consent as it was to give consent in the first place. Additionally, if companies change their terms and conditions they cannot always rely on the same consent. All processing operations that date from prior to the application of the GDPR have to be in accordance with the GDPR (i.e. companies need to revise the consent obtained before the GDPR and possibly ask for it again). As a final note, the **lack of alternatives** to the consent requirement was mentioned. It was stressed that the requirement in itself is not bad, but that it is the implementation which is problematic.

Questions raised:

- *What will be the effect on legal certainty if there are not only different ages among different Member States, but also the possibility of changing ages with changing governments?*
- *What is the role of NGOs at national and EU level in relation to the enforcement and implementation of the Regulation? Specifically, could litigation be initiated by NGOs in order to hold the industry accountable?*
- *How could children be better protected and how can data protection impact assessments take children's interests into account?*
- *How do companies implement the requirement to prove that they have adopted reasonable measures to verify a child's age? Are companies collaborating on the creation of feasible methods and what is the state of the art of the current technological possibilities? Are consumer organisations cooperating with companies on the technological issues?*
- *Could 'privacy dashboards' be adopted to allow user to give consent more granularly?*

- *How will data controllers verify whether the consent they have already obtained is in accordance with the GDPR requirements and how will they obtain 'fresh consent' if necessary?*

Session 6: Article 8, parental consent and codes of conduct

Moderator: Patrick Geary (UNICEF)

Definition of an 'information society service' 'directly offered to a child'

It is unclear what constitutes an 'information society service' 'directly offered to a child' in the context of article 8. The definition of an 'information society service', which has its origin in existing EU Directives, is "*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*". The fact that a service is advertising-based and does not charge a fee to the user does not exclude a service from this definition. However, it is not clear whether services offered for instance by non-profit organisations will, in all circumstances, fall outside the scope of article 8 GDPR.

Furthermore, the question was raised whether the second element of this notion means that article 8 GDPR only applies to **services specifically targeting young children**, for instance YouTube for Kids? Or does this refer to services that are used by children, although they are not specifically targeted to them (e.g. Facebook, eBay)? It was suggested that **actual research with children** could provide clarity on which websites are the most popular ones among children of a certain age. Looking at **COPPA**, two important elements are taken into account: (1) services targeted at children and (2) operators having actual knowledge that a service user is under 13.

An interesting point was made in relation to **article 24 GDPR** which requires every data controller to consider if there are any risks associated with that processing of personal data. It was argued that providers will not be able to implement this provision unless they know who their customers are exactly. Simply stating that services are not directed at children should not be sufficient. In other words, **the idea of knowing one's customer must form part of the responsibility of every information society service provider**. Yet, also in this context, the data minimisation principles needs to be complied with. Crucially, it was argued, **the backbone of the GDPR is the identification of vulnerable persons and the protection of their fundamental rights.**

Advertising-based business models

Different views were shared concerning the **advertisement-based business models** of online services. On the one hand, it was suggested that it is feasible to offer social media services without a business model based on the collection and selling of personal data for advertising purposes. Industry representatives, on the other hand, stressed that there are costs associated with the services and content produced. Furthermore, even if such services were to be provided for a charge but with no advertising, processing of personal data would still form part of the service because of the need for updates and the personalisation of services. It was finally

stressed that there is **no problem with advertising-funded services, but there are problems associated with a certain type of business models**. Modern business models are often incomprehensible for children as well as adults. There is a major difference between, for instance, Spotify giving recommendations based on user preferences and selling this information to third parties for marketing purposes.

Which verification mechanisms will be accepted?

Existing methods and technologies are mostly based on providing proof that a user is over 18 years old (e.g. ID cards, credit cards) but most EU countries do not actually have a trustworthy system, especially not for younger children. However, it was stressed that simply because a good technological solution for age verification of children does not exist right now, it does not mean that it cannot be invented in the near future. The DPAs of each Member State **will have to provide guidelines** on the solutions and approaches that are compliant with the GDPR. Perhaps a mechanism with trusted third parties and digital tokens could be used (i.e. no name or credit card data would be required).

Finally, doubts concerning the desirability of age verification as opposed to the **idea of anonymity on the internet** were expressed. We are moving very quickly to an environment in which everyone has to be identifiable at all times. Age verification should not become a negative catalyst in this context.

Questions raised

- *What is an 'information society service' 'directly offered to a child'?*
- *Will services offered for instance by non-profit organisations always fall outside the scope of article 8 GDPR?*
- *Does article 8 GDPR only apply to services specifically targeting young children, for instance YouTube for Kids? Or does this refer to services that are used by children, although they are not specifically targeted at them (e.g. Facebook, eBay)?*
- *Which parental consent and/or age verification mechanisms will be accepted?*
- *Is age-verification desirable in the context of anonymity on the internet?*

Session 7a: Profiling, behavioural marketing and data protection impact assessments

Frederik J. Zuiderveen-Borgesius (University of Amsterdam), David Martin (BEUC), Jeff Chester (Center for Digital Democracy)

Moderator: Anna Fielder (Privacy International)

As a first question, the panellists were asked about the **impact** of profiling and behavioural marketing on individuals' rights. According to one of the panellists, the question that needs to be asked is whether we want our children to grow up in a **commercial surveillance world**, with cross-device tracking and targeting, advertisements changing in real time, the rise of applications designed to bypass rational behaviour (i.e. neuro-marketing) and the establishment of huge data broker vehicles and marketing clouds. Essentially there are two

processes: (1) the old-fashioned mathematical statistical process where people are profiled in categories and (2) the new phenomenon of big data analytics which uses machine learning which constantly adjusts profiles according to consumer behaviour. The latter can be inaccurate, different (depending on how the algorithms are built) and even discriminatory. Accordingly, it can **impact children's wellbeing and self-image** (e.g. unhealthy food).

Several panellists and roundtable participants stressed that **certain practices should be simply off limits for children under a certain age**. This requires a granular discussion about children's developmental capacities. Additional safeguards are needed, for instance through specific sectorial regulation on privacy or an articulation of what the best practices relating to children should be. Notably, these safeguards should not limit children's participation and should be based on children's rights. Furthermore, with regard to profiling and targeted advertising it is important to note that according to article 7 (4) GDPR, consent cannot be tied to data which is not necessary for the provision of the service (e.g. targeted advertising). **Perhaps the fairness principle can be used to tackle such practices**.

What are 'legal or similarly significant effects'?

Recital 71 of the GDPR provides typical examples of what may constitute a legal effect for adults (e.g. in relation to credit applications). However, what could this mean for children? Participants agreed that the importance of article 22 really depends **on how one interprets "*produces legal effects or similarly significantly affects*". If behavioural advertising falls under this notion, the impact on the industry could be extremely significant.** On the other hand, if the bar is high then the effect will be minimal. One participant believed the threshold should be quite high, considering recital 47 GDPR which provides that processing for direct marketing purposes may constitute a legitimate interest of the controller. It is worrying that only 11 months remain before the Regulation is applicable and there are still no clear ideas on the implications of the rules.

Are there any alternatives?

An industry representative argued that, with the algorithms today, one could to some extent provide children with a similar experience **without collecting their personal data**. Children do not actually want to share their data, they just want to have access to content. Companies do not have to rely on profiling. They could instead gather broader knowledge about user groups and move outside of the personal scope.

How can children's views be included?

A participant shared that research has shown that children themselves are aware that not all the data they are being asked to share is needed for the use of the service. They also expressed their willingness to decide themselves whether they wanted to see an ad or not. Furthermore, as regards child participation, it was mentioned that in certain countries, for instance in Denmark, there is a long tradition of **organising children panels.** In this regard, workshops with high-school students on privacy showed that while they understood privacy in a social context (i.e. towards their peers or parents), they did not know much about privacy in a commercial context (i.e. towards companies).

Questions raised:

- *What is the impact of profiling and behavioural marketing on individuals' rights?*

- *What are 'legal or similarly significant effects'? What could this mean for children?*
- *Are there any alternatives to business models based on data collection?*
- *How can children's views be included?*

Session 7b: The implications for data protection and privacy education

Prof. Gloria Gonzalez-Fuster (VUB), Prof. Simone van der Hof (Leiden University), Pascale Serrier (CNIL) and Jeroen De Keyser (National Support Service eTwinning)

Moderator: Hans Martens (European Schoolnet)

The participants in the session were divided into four different groups along with the panellists for a more in-depth engagement and a thorough discussion of the specific needs and challenges from the perspective of data protection and privacy education. Participants discussed **possible future initiatives, measures and their implementation in practice**.

The need for trust in educators was emphasised, as well as trust in children themselves. It became apparent that many teachers are unaware of data protection implications. Teachers are not being trained in that sense. Perhaps it should become compulsory for educators to make sure that, by a certain age, children are educated on such issues as data protection.

The implementation of privacy-enhancing methods and digital literacy should not only focus on risks and the protection of children but also on empowering them by building their skills and understanding. A key issue is to find a balance between (merely) 'protecting' children and helping them to participate in online activities; an excessive emphasis on 'safeguarding' can lead to the wrong framing of the issues as stake, putting too much stress on 'risks' as opposed to 'rights'. Rather, online safety should be understood as a component of a wider concern with digital competence, which would take as starting point the experiences and expertise of children.

Another challenge involves the difficulties of teaching children about the long-term consequences of sharing their data as they often seem not to be concerned about it. Young people and children should be involved in this discussion. They should be made to care about data protection without focusing too heavily on the abstract concepts and the technicalities of it as it may be too difficult to understand (and too boring).

It was agreed that parents – just like teachers – often lack the required skills in terms of privacy and data protection, which can make their children more vulnerable. Children, in spite of being somehow digital natives, do typically lack the knowledge and maturity to fully understand the implications of certain behaviours and developments, so a dialogue between all relevant actors is critical.

Participants identified the following **solutions and action points**:

- Making **data protection and privacy education an obligatory part of the curriculum**, involving all teachers, staff and the school management on the topic, while integrating it across other subjects.
- A right to learn about data privacy/protection issues, and a system to support it should be implemented. Within this context, more attention should be given to corporate surveillance and unfair commercial practices.
- A fair balance needs to be struck between the legitimate interests of some companies in delivering certain technologies for children and the interests and rights of minors. This is particularly relevant in light of the current spread of Learning Analytics and Artificial Intelligence technologies for and in schools.
- Immersive games on 'data dealing' could be created where pupils learn more about the process of acquiring and selling data, thus, developing a better understanding of how data commercialisation works.
- Resources, training and guidelines, including easy-to-use videos and online project, should be developed to teach different stakeholders about e-safety, digital literacy, privacy and data protection. In schools, a dedicated ICT coordinator should be appointed to initiate more meaningful data protection projects. Privacy activists, including NGOs, can be instrumental in contributing to general awareness of privacy and data protection issues.
- Involving industry is a must and schools cannot do it on their own. Thus, partnerships between schools, children's rights organisations, industry, parents' rights organisations and education networks such as European Schoolnet should be nurtured.
- As a possible solution for children lying about their age, instead of restricting children's access to services if they are under 13, access could be offered to other services, either a free subscription to a similar service or a 'growing account' possibly attached to the parents' account (for instance, in case of social media platform, more features could be made available as the child grows).
- Scores based on data protection impact assessments could be published on websites.
- Questions concerning future guidelines should be raised with DPAs and stakeholders to clarify issues that should be dealt with in the future.

Questions raised:

- *From a data protection and privacy education point-of-view, against the background of the GDPR, what are the key issues, needs and challenges?*
- *What are possible future initiatives, measures and their implementation in practice in terms of data protection and privacy education?*
- *Who should bear the responsibility for children's privacy and data protection education – parents, teachers, schools?*
- *Are teachers aware of data protection implications and can they help in teaching children about privacy and data protection? Are they trained enough for that? Who will teach the teacher?*
- *Which role will be played by DPAs in this area?*

Agenda

9.30-10.00	Arrival, coffee & registration (*Room 6306*, 6th floor)
10.00-10.05	Welcome & introduction Hans Martens (European Schoolnet) & Eva Lievens (Ghent University)
10.05-10.30	The GDPR: history, rationale and future guidance Karolina Mojzesowicz (European Commission)
10.30-11.00	Identification of children's rights issues in the implementation of the GDPR in practice Eva Lievens (Ghent University) & Simone van der Hof (Leiden University)
11.00-11.30	Do children understand the commercial nature of the internet? Sonia Livingstone (LSE)
11.30-12.00	Experiences from the United States & COPPA Kathryn Montgomery (American University)
12.00-13.00	Challenges for DPAs, industry, parents and children Moderator: Peggy Valcke (KU Leuven) - *Caroline De Geest (Belgian Privacy Commission)* - *Andrea Parola (ICT Coalition)* - *David Martín (BEUC)* - *Vicki Shotbolt (Parent Zone)*
13.00-14.00	Lunch
14.00-15.00	Article 8, parental consent and codes of conduct Moderator: Patrick Geary (UNICEF) Questions include: - *Which services will be classified as 'information society services' 'directly offered to a child'?* - *What age will be chosen in which countries on the basis of which processes?* - *Which practical challenges will arise if different ages are maintained throughout the EU?* - *Will 'fresh' consent need to be obtained to continue processing activities that do not fulfil the GDPR standard?* - *Which verification mechanisms will be accepted?* - *Who will take the initiative to draft codes of conduct?*

	- *Which other legitimation grounds can be used to process personal data of children aside from consent?*	
15.00-16.15	Profiling, behavioural marketing and data protection impact assessments (Room 6306) Moderator: Anna Fielder (TACD, Privacy International) Panellists: Frederik J. Zuiderveen Borgesius (University of Amsterdam), David Martín (BEUC), Jeff Chester (Center for Digital Democracy) Questions include: - *Is profiling prohibited for all under18s?* - *Is profiling only prohibited if the decision has a legal or other significant effect? Which decisions vis-à-vis children would qualify as having such an effect?* - *Which measures will / need to be adopted to provide 'specific protection' to 'children'?* - *Should there be default limitations on the collection of children's personal data for profiling or behavioral marketing purposes?* - *Will different measures be adopted for different age groups?* - *When do data controllers have to carry out a DPIA? To what extent and how should children's own views be incorporated in such an assessment?*	Implications for data protection and privacy education (Room 4402) Moderator: Hans Martens (European Schoolnet) Panellists: Gloria Gonzalez-Fuster (VUB), Simone van der Hof (Leiden University), Sophie Vulliet Tavernier (CNIL), Pascale Serrier (CNIL), Jeroen De Keyser (National Support Service eTwinning) Questions include: - *Which role can/should DPAs play in raising public awareness of the data protection risks, rules, safeguards and rights in relation to children?* - *How is data protection/privacy currently integrated/referenced in national education policies and actions?* - *Which learning and teaching frameworks, resources and campaigns exist, as developed by data protection authorities, Insafe network members and other civil society organisations?* - *What are the GDPR implications for schools, particularly in regards the use of information society services?* - *What is the perspective of teachers, in terms of the type of support and guidance they may need?*
16.15-16.30	Lessons learned and steps forward	Lessons learned and steps forward

Acknowledgements

Rapporteurs

Ingrida Milkaite (Ghent University)
Valerie Verdoodt (KU Leuven)

Logistics and Social Media

Fiorella Belciu (European Schoolnet)
Sabrina Vorbau (European Schoolnet)
Teodora Garbovan (European Schoolnet)
Koen Glotzbach (European Schoolnet)
Mirela Gica (European Schoolnet)

Organising Committee

Hans Martens (European Schoolnet)
Eva Lievens (Ghent University)

With support from

For any further queries

Please contact gdpr-roundtable@eun.org.