LSE MEDIA POLICY PROJECT Promoting media policy communication between academics, civil society & policymakers

What does the European General Data Protection Regulation mean for children in the UK?

Report on an LSE Media Policy Project roundtable

On 20 November 2017, a roundtable discussion chaired by Sonia Livingstone was held at the LSE to explore how the European General Data Protection Regulation's new requirements will affect both children and the organisations that process their data. It built on a previous discussion held soon after the GDPR was published, and began the consultative process for the Information Commissioner's Office (ICO) guidance by identifying a range of issues, priorities, common ground and differences of opinion.

This short report focuses on the key points and issues that arose. Representatives from various sectors were invited to participate in the meeting, and they are referred to by sector in this report: the Information Commissioner's Office (ICO), academia, NGO, consumer advocacy, legal opinion, intergovernmental organisation (IGO), and Industry.

Chatham House rules applied.

The context

In May 2018, the GDPR will introduce important new data protection requirements with respect to the processing of children's personal data. For the first time, there will be an explicit requirement that children's data must be given specific protection, particularly when an organisation wishes to collect their data, use it for profiling purposes or send them marketing. There are also significant new considerations for an organisation when it offers an 'Information Society Service' directly to a child and wishes to obtain consent for processing any personal data collected.

The Information Commissioner's Office (ICO) began the event by explaining its current thinking about the implications of the GDPR - both for children, and for organisations processing their data.

In her introduction, the chair noted that although efforts to interpret and implement the regulation have been widely debated, the position of children remains both unclear and relatively little discussed – notwithstanding some publicity surrounding Article 8, the age at which a child is judged capable of consent. Legal interpretations already seem to differ on a range of issues relating to children (and more generally), including the legitimate bases of processing data, jurisdiction, the need for risk impact assessment and rules on data profiling. A host of practical questions remain unresolved, including those concerned with age verification, obtaining consent from parents and ensuring transparency and compliance.

The protection of children's personal data under the GDPR

ICO

→ Recital 38 of the GDPR says children merit specific protection because they may be unaware, or less aware, of risks, consequences and safeguards regarding their personal data. Data controllers, when considering the general approach to processing children's personal data, should think about

transparency and children from the outset. We recommend they take a risk-based approach, carrying out an impact assessment of data protection and data minimisation.

→ Bases for processing: A general misconception is that consent is the only basis for processing data concerned with children. Article 8 indicates that is not. One of the benefits of GDPR is that it forces data processors to be upfront about their basis for processing. GDPR also highlights that data processors should make sure a child is competent to contract.

→ Legitimate interests: A balancing act between the interests of data controllers or third parties and the interest of a child is required.

→ Consent and risk assessment: Consent can apply both generally and in the specific context of article 8. Risk assessment is recommended for consent as well. Even if data processors go through consent, they still have a responsibility to look at what they can and cannot do. Similarly, marketing to children is not prohibited by GDPR. However, data controllers are required to comply with all the requirements in GDPR.

→ Profiling and automated decision making: Recital 71 says automated decision making should not concern a child. However, it is a recital and not in the article. A Working Party 29 opinion on profiling and automated decision-making has indicated that data controllers need to be transparent when they are profiling. If they do profile, the case has to fit one of the permitted circumstances in which they can do so, and they need to make sure adequate safeguards are in place.

→ Privacy notices: The notices should be written in clear language, particularly when they deal with children. Consent must be informed.

→ Rights and competence: A parent might want to exercise the rights on behalf of a child if he or she is too young to understand what they are. If a child understands what the rights mean, then it is the child who should be exercising them. In cases where parents and the child want different things, GDPR does not assume parents take precedence, providing the child is competent to understand that it is their rights.

Key questions regarding the GDPR

ICO

→ **What is a child?** Anyone under the age of 18. Neither UK nor European law define what a child is. The UN Convention on the Rights of the Child says it is anyone under the age of 18, unless majority is attained earlier under national law around the world. GDPR intends to protect anyone under 18.

→ **What is an information society service (ISS)?** An information society service is not necessarily something that the end user is paying for. It might be paid for in some other ways, such as through advertising. If an online service is offered indiscriminately - for instance, without an indication that

children should not access it – then it is also considered a service provided to children. If a service states that it is 'only for people over 18' or 'adults only', then the process of looking for evidence will be carried out to ensure that the restriction is put in place in practice, not just in theory.

→ **Do ISS providers have to age verify all children?** If they rely on consent as a basis for processing, and provide services directly to children, the answer is yes. The implication of article 8 is that the service providers will have to conduct age verification. A risk-based approach is recommended here.

→ **How can the age of the child be verified?** GDPR has not worked out the answer to this question yet. Co-ordination with the marketplace is needed. Some presume that if social media companies can target advertising based on a user's profile, then they must also know how old someone is. This is an interesting point: if a service provider has to profile someone in order to verify their age, can the provider actually do that? The guidance has not answered this question. ICO assumes responsibility for this area is 'over to the marketplace'. Verifying parental consent is an even more difficult question. Article 8 says service providers have to use reasonable efforts and available technology to verify that the person giving consent on behalf of a child who is under the age of consent holds responsibility.

→ **Can children be profiled?** This question has been considered in the Article 29 Working Party, which has published its opinion (pdf document). The answer is yes, but sufficient safeguards must be in place. The automated decision-making provisions apply to decisions based on the processing of children's personal data which produce legal – or similarly significant - effects concerning them. There is debate about what 'similarly significant effects' are. When companies are profiling children or making an automated decision, often they are trying to influence children's behaviour. During that process, they need to consider what it is that they are trying to make the children do and how they are trying to influence children's decisions.

Concerns and commentary

Legal opinion

→ Participants agreed with ICO's point about the importance of writing privacy notices in clear language so that children can understand them. Additionally, they said ICO's effort to draw on the experience of other fields (such as advertising) is a good approach, since the online world, unlike other sectors, does not treat adults and children differently. The questions of how to verify age and parental consent need to be addressed. They expressed concern over ICO's assumption that these questions are 'over to the marketplace'. The marketplace has not dealt with Internet safety issues properly: bodies like ICO must lead the way in finding solutions.

Industry

→ Participants agreed with the principles of the GDPR, and its focus on creating practical guidance for businesses. They called for more clarity to help companies do the right thing. Concerns were raised about how stringent requirements for age verification and parental consent could restrict children's access to age-appropriate content compared to other sites. It is crucial to ensure the sector can keep providing content for children. For that, it needs to understand parental consent and how much data needs to

be collected from parents.

Age verification tools

Academia

→ PAS 1296 is a framework for evaluating age verification solutions. It does not solve the problem of how to verify age, but it does give the opportunity to evaluate the solutions available, what kind of data to use and the security processes involved.

NGO

→ In Germany, age verification solutions are certificated. They prove a person is over a certain age. With GDPR, however, something that helps to prove a person is under a certain age is required. The age verification issue cannot be solved by the market alone. Two possible solutions exist: a reliable form of child ID, or employing a trusted third party.

Industry

→ 'Digital Policy Alliance', a cross-party group working on age verification, has been launched. There exists an age verification solution which proves a child is under 18 and is linked to a government-issued ID.

→ Trusted third-party solution: **Industry** believes a two-stage solution involving a trusted third party has advantages, since the company providing the service does not hold the data, but entrusts the processing to a third party. Are there ways to promote this type of solution? In response, **ICO** indicated they prefer a solution that does not require data controllers themselves to keep personal data, but other approaches are not ruled out. **Trade association** expressed concerns that one trusted company might become a monopoly, forcing companies to pay. This would be particularly difficult for SMEs.

Data impact assessment and age verification

→ **NGO** and **ICO** agreed that data impact assessment is a useful tool. Additionally, **NGO** pointed out that if a service offered without specifying age is deemed to be provided indiscriminately, every service becomes liable for data impact assessment in relation to its consequences for children.

Academia

→ Does every service needs to verify age? **ICO** replied that article 8 only applies when a service is offered directly to a child. A provider may not offer children its services directly, but in practice it needs to prove that its service is not available to children. In other words, service providers may end up verifying age anyway. **NGO** said risk assessment could be a solution, and obligation is contingent on the risk assessment. Another **NGO** and **Industry** disagreed that the obligation should depend on

the result of the risk assessment. Obliging every website to verify age may not be the intended consequence of Article 8. Moreover, **NGO** stated that Article 29 should be discussed at the European level. While agreeing on a risk-based approach, **NGO** also suggested industry and ICO should have an open discussion about how best to verify age.

→ Data minimisation: **NGO** asked 'if a service is offered indiscriminately, does it mean that the service is provided to a child?' If so, every single website should have a tick box for age verification. The **NGO** said recital 57 should not be forgotten. The article is about not collecting personal data other than that needed to identify a person. A service does not need to ask how old a person is for age verification. All it has to know is whether a person is under a certain age. Regarding the 'certain age', **Academia** and other **NGOs** agreed that there are two attributes for age verification: 'under 18' and 'under 13'.

→ **NGO** questioned why it is such an issue if every website verifies everyone's age. **Academia** responded that it is problematic as it is both a privacy and security issue - an unnecessary collection of data, with the risk of data leaking and hacking.

→ **NGO** brought up the topic of using age verification to get contents removed. It must not be easier to share contents than to get them taken down. The age verification debate is as much about what the 'right to erase' means as the right to use, upload and share content. Another **NGO** pointed out that age verification is not intended to be around content. Article 8 of the GDPR is about how service providers use data collected from children. Nonetheless, most of the participants concurred with the idea that verifying one's age in order to take contents down should be no more complex than the verification process for accessing a website.

→ **Consumer advocacy** pointed out that the US system of age verification is no more sophisticated than the UK's. Most of the time, it involves either ticking a box or supplying a date of birth. It is common practice for parents to tell their children to lie by saying they are over 13. This has implications for the UK because a lot of UK children use US websites (where COPPA applies). **Consumer advocacy** agreed with ICO that connecting what other rules say about **profiling** is important. One of the major reasons for profiling children is to target them with food advertising, which may have a significant negative impact on them. The guidance on profiling is therefore important because it will imply collaboration between different sectors.

Internet-connected devices

→ **Academia** questioned how is ICO going to deal with internet-connected devices used in the home these days, given they are mostly not screen-based. **NGO** agreed with **Academia**, pointing out that whatever will pick up children's personal data in the future will not be screen-based. GDPR's design does not address that issue.

Consumer advocacy

→ Smart toys and consent: **Consumer advocacy** asked at which point consent should take place

when it comes to smart toys. **Trade association** responded that guidance on connected toys has been released, but complexity still exists. Businesses are advised to get consent from the very beginning, before customers start using the product. In addition, companies are advised to be transparent about the kind of data they are collecting and how it is being used. Long lead times in toy development means it will be 12-18 months before current thinking becomes apparent in the market.

→ **Consumer advocacy** were concerned that children's smartwatches can be hacked. Horizontal legislation on the basic security of such products might be needed. Furthermore, the complicated value chain involving producers, importers, retailers and so on is an issue: which of these will take the liability? Some are not even members of trade associations. They are small and not aware of the guidance. **Academia** pointed out that social media and websites do not even have industry associations. How is ICO going to reach them and ensure they all comply? **ICO** responded that it reaches out to them through engagement, guidance and enforcement actions, if necessary.

The Article 29 Working Party and protecting children's data

NGO

→ Ten guidance notes are being issued by the Article 29 Working Party. Two are out for consultation now, and five have been agreed. Another three will follow. **NGO** asked if one of those three will be on children. The answer was 'no'. In response, **NGO** stated that the Article 29 Working Party and the Commission have a legal obligation to try to ensure consistency in implementation of the GDPR. How will this happen if they are not going to indicate how that consistency is going be determined? **NGOs** pointed out that the Commission only issues two sets of guidance a year and has programmes of priorities. The group prioritises a certain agenda by looking at Europe-wide issues. So far, the work programme has not included anything specific on children. Academia, NGO and other participants agreed that 'more noises are needed.'

→ **NGO** said ICO's guidance would be very useful in pushing other countries to have similar conversations. 'Making noise' would also be essential to ensure people realise issues regarding data protection and children are more problematic than they have assumed.

Implementation of the GDPR

→ **Industry and NGO** raised a question regarding jurisdiction. Countries have different age standards and laws. **ICO** said it is waiting for a consent opinion from the Article 29 Working Party. ICO current thinking is that if a service is offered in the UK and targets UK children, it is subject to UK rules. Asked 'If a child lives in one country and is registered to a service in another, which country's law should apply?', **ICO**'s answer was 'the law in the country providing the service a child signed up to', but added that this is not clear-cut.

Other participants pointed out that when it comes to marketing, regulators expect you to follow the rules in the country where the person receiving the marketing is based. The Article 29 Working Party consent guidance confirms this view (pp24-25). There have been several court cases on applicable law, and having a presence in other countries makes their law apply. It defeats the object of each

country setting their own consent age for online service providers if you only apply the law in the country you are in. That would mean US providers using 13, which is not what was intended by article 8.

→ Practical challenges: **Industry** pointed out a practical challenge to article 8. Hypothetically, if a child could be registered to a service at the age of 13. After May 2018, they might be in a situation where they could not obtain parental consent. In this case, what should a data controller do? If a child can no longer use a service because of this problem, it is not only a legal issue but an emotional one for children.

→ Legitimate interests: As a charity, **NGO** is looking at whether it could hold data on children, under legitimate interests rather than consent. Article 9(d) provides grounds for that. However, the status of charities is unclear. **Data protection expert** added that a current provision for charities is carried over into the UK draft data protection bill and the basis of the law is not going to change.

→ **NGO** raised a question regarding recitals. Recitals are not binding, and not all of them will be included in the article. So what is their value? **ICO** responded that recitals have interpretive value. Articles address intention.

Topics in need of more attention

IGO

→ Once children are above the age of consent, their data is treated like adults'. This should not be the case. Service providers can give separate terms and conditions to children above the age of consent. **Academia** agreed that children aged 13 to 17 look relatively unprotected.

Academia

→ While discussing protecting children's data, it is important to note that the products and services under scrutiny offer children freedom of expression, as well as being valuable and enjoyable.

Legal opinion

→ Pointed out the lack of funding for children and their data protection. There should be more investment in the vital issue of children's safety and wellbeing online.

Conclusion

The ICO and representatives confirmed they agreed on some issues, but some contested topics need further discussion.

A post about the GDPR will be published on the LSE Media Policy Project blog shortly.

Further information

ICO - About the GDPR
ICO: European guidance on profiling and breach reporting
ICO - Data Protection Bill
Digital Policy Alliance Age Verification & Internet Safety Page
Proposed Amendments Led by Baroness Kidron - Minimum Standards of Age Appropriate Design into the Legislation
Child Line - Enabling a Young Person to Share an Under 18 Token
2016 General Data Protection Regulation Roundtable Meeting Report