UK Consultation[1] on General Data Protection Regulation derogations

Summary of Recommendations

"With its 173 recitals and 99 articles, the GDPR is a very extensive piece of legislation which covers many topics, obligations, sectors and actors. It seems clear that children and their rights have not been thoroughly considered in the course of the data protection framework review process." (Eva Lievens, Professor of Law and Technology at the Law Faculty of Ghent University)[2]

The UK now has an opportunity to offer a positive and inclusive step to our young people, and consider their views on legislation which will affect them for their foreseeable lifetime. The UN Convention on the Rights of the Child emphasises that children's views should be heard and given due consideration within the family and in schools[3] including *"from the most marginalised communities."* However this consultation has not offered them a way to do this.

It is also vital to get this right for the education and commercial edTech sectors, as noted in the UK Digital Strategy.[4] Derogations include use of sensitive data and biometrics. Technologies capturing these data are becoming increasingly used for children where they are not for adults, widespread in school canteens and libraries, and we would welcome the opportunity for greater in depth discussion to ensure the derogations capture the required nuances to protect both future technology and economic interests, as well as the rights of the child.

We recommend that

1. a separate consultation be undertaken with regard to the effects of GDPR and derogations on the rights of children, if the am of this exercise is *"to capture views on if and how the government should implement the defined flexibilities permitted within the GDPR*". The current consultation without proposals set out, without any supporting background information, and under one month timeframe given, cannot achieve this purpose.

2. Overall, derogations must ensure that Recital 38 and Article 6 (2) (f) are applicable and upheld for all children (i.e.until the age of 18). Additional protection measures will need to be adopted for children between the chosen age of consent under Article 8 and legal maturity at 18, especially with regard to opaque privacy-intrusive practices in information society services (online) and how parental 'consent' might affect child rights under Article 17(f).

3. Any code of conduct, under Article 40, should ensure explicit protection of the rights of the child of all ages and the regulation overarching approach to fundamental rights and freedoms and the respect of children as 'vulnerable' and merit specific protection in Recital 38. The manner in which age and consent verification is obtained must therefore not be more intrusive on privacy or permanent regards use of their online behavioural data, than would have been, were it not required. Mechanisms and terms must be transparent and easily understood by parents and children.

4. Regards articles under theme 10, it needs specific further consultation as regards children given the complexity. This includes profiling and should take into account the responses and conclusions of the ICO consultation which has not yet been published. The ability to enact the right to erasure is of particular importance to children.

5. As regards Article 8, any lowering of the age verification requirements should be made on a research evidence based approach. This may mean the age is lowered from sixteen to enable freedom of access and rights to participation, but must not stand alone. The risk is that lowering the age to 13 as a stand alone step, could mean 13 year olds effectively treated as adults[5] and not offered the consideration they merit acknowledged under Recital 38.

6. Ongoing discussion is needed here involving civil society, children's advocates and open to young people themselves. Parents cannot consent on behalf of a child, they merely assume responsibility for the method and its effects. Some will be unable or unwilling to do so for access which will lead to children finding workarounds. There must be mechanisms in place that ensure other derogations and regulations are respected for all children of all ages including transparency of processing, right to erasure, understanding profiling, and full inclusion of young people.[6]

---

[1] https://www.gov.uk/government/consultations/general-data-protection-regulation-call-for-views

[2] http://blogs.lse.ac.uk/mediapolicyproject/2016/11/10/wanted-evidence-base-to-underpin-a-childrens-rights-based-implementation-of-the-gdpr/ LSE Media Policy Project "Wanted: evidence base to underpin a children's rights-based implementation of the GDPR" accessed May 9, 2017

[3] https://www.unicef.org/southafrica/SAF_resources_crcgeneralcomments.pdf p41 para 50

[4] https://www.gov.uk/government/publications/uk-digital-strategy

[5] https://medium.com/@janicerichardson/european-general-data-protection-regulation-draft-the-debate-8360e9ef5c1#.616jqhj4q Janice Richardson, expert to ITU /Council of Europe

[6] ibid Para 30 CM/Rec(2013)2. 1.2. Countering discrimination

Introduction

This consultation[7] with under a month to respond is insufficient opportunity to comment on the required derogations that affect children and gather their views, or those of children's organisations that will be affected but do not normally follow Data protection legislation. There are still questions and academic research[8] being undertaken that offer evidence based insights which should be considered. We recommend that the upcoming work of whose work[9] is specific to GDPR and children is also taken into consideration, expected after this closing period, plus the extensive research[10] by and .[11]

Involving children in decision-making at individual, family, organisation and policy level in society is key to realising their rights. While our young people's future ability to live and work in Europe may become more limited than it is today, we should ensure their ability to participate and collaborate online is not. The Council of Europe Strategy on the Rights of the Child[12] 2016 - 2021 *Right to be Heard (Article 12)*, *aims on Non-discrimination, and Freedoms to develop fully (Article 6)* are important to consider in the derogation of GDPR Article 8, on which we focus in this response. But children and their supporting organisations will not have been able to respond to this consultation as it is.

The Strategy makes specific mention on the rights of adolescents to have their own views taken into account.[13]
It also notes that, *"Digital tracking and surveillance, the collection of personal data, including sensitive data related to health, for the purposes of profiling pose a threat to privacy and the general enjoyment of human rights including freedom of expression and access to information."*

UK derogations must ensure to be privacy enhancing not harmful to young people. We must balance age-based restrictions intended to protect children from content with ensuring participation information access are not limited.

Parental financial limitations should not be passed on a child which restricts their relevant freedoms of cultural and civil rights, and the State should strive to ensure the widest possible enjoyment of rights.[14] This is of consideration if the derogation/ codes of practice were laid out that in practice lead to methods that require credit card data for example.

There are a number of important potential areas for improvement in how the GDPR derogations will affect the rights of privacy and data protections for children. Implemented poorly, a number of these also pose increased risks instead, including through the complexity of the implications of the age verification and consent requirements in Article 8.

Who is a child?

The GDPR has no definition of the age at which children are deemed to be competent, or at what age childhood ends. Boundaries in this sphere are arbitrary. However, *"The evidence does not, [therefore], give a ringing endorsement for those aged 13+ to use the internet at will."*[15] *[Professor Sonia Livingstone, LSE Media Policy Project, 2016]*

This is fundamental to consider across the application of the GDPR but specifically with regards to Article 8 and a child's consent provision of information society services. The requirement to provide parental consent and age verification in GDPR is problematic in many areas. It could lead to greater risk of data exposure and exploitation of a child's identity and tracked behavioural data.

Research from the Nuffield Foundation on the age of digital consent by Terri Dowty and Douwe Korff in 2009[16] includes international comparisons, many of which hold true today. They concluded, "*a child's age is not relevant to consideration of their competence to consent. Competence depends on the maturity of the child; the quality of the information provided to them; the nature and sensitivity of the data; and the child's understanding of the purpose(s) for*

---

[7] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/610133/EnglishGDPRCFV_v1.5.2pdf_2.pdf

[8] http://blogs.lse.ac.uk/mediapolicyproject/2016/12/12/the-gdpr-using-evidence-to-unpack-the-implications-for-children-online/

[9] https://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=566731

[10] http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20I%20(2006-9)/EU%20Kids%20Online%20I%20Reports/EUKidsOnlineFinalReport.pdf

[11] https://www.liverpool.ac.uk/risk-and-uncertainty/staff/savirimuthu/

[12] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168066cff8

[13] https://www.unicef.org/southafrica/SAF_resources_crcgeneralcomments.pdf page 31 paragraph 32

[14] https://www.unicef.org/southafrica/SAF_resources_crcgeneralcomments.pdf p36 paragraph 8

[15] http://blogs.lse.ac.uk/mediapolicyproject/2016/12/12/the-gdpr-using-evidence-to-unpack-the-implications-for-children-online/

[16] http://www.nuffieldfoundation.org/sites/default/files/Protecting%20the%20virtual%20child.pdf Protecting the Virtual Child, Nuffiled Foundation, 2009 (Dowty, Korff)

which the data are shared, the organisations or individuals who will have access to their data and the consequences of consent, or of failure to provide it. it requires careful assessment of each individual child."

The Council of Europe 2016-21 strategy on the rights of the child makes clear that all children's rights during childhood are considered equal and views given due weight, until adulthood at age 18, "*Children have the right to be heard and participate in decisions affecting them, both as individuals and as a group. Indeed everyone has the right to freedom of expression, as guaranteed under Article 10 of the European Convention on Human Rights. The UNCRC grants children the right to express their views freely in all matters affecting them and to have their views given due weight* ***in accordance with their age and maturity.*** *"*[17]

Recommendation: Legislation must ensure that Recital 38 and Article 6 (2) (f) which are applicable to all children (i.e.until the age of 18) are not undermined by the application of any age reduction made under derogation of Article 8.

Theme 3: Demonstrating Compliance

Article 40: Code of Conduct (2)(g): Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:

the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;

We suggest that any code of conduct should ensure explicit protection of the rights of the child of all ages and the regulation overarching approach to fundamental rights and freedoms and the respect of children as 'vulnerable' and merit specific protection in Recital 38. The manner in which age and consent verification is obtained must therefore not be more intrusive on privacy or permanent regards use of their online behavioural data, than would have been, were it not required. These mechanisms and terms must be transparent and easily understood by parents and children.

Theme 9: Rights and Remedies (with reference to Right to Erasure)

Article 17: Right to erasure
Article 22 - Automated individual decision-making, including profiling

Case study: Tiziana Cantone had won a "right to be forgotten" ruling in Italy - but the court had ordered her to pay €20,000 (£17,000; $22,500) in legal costs.[18] Recital 65 sets out that this right is especially relevant when a child consents to processing and later wants to remove the information, even if he is no longer a child. How Article 17(2)(f) may be affected by derogations in Article 8, should be considered as well as limitations in 17(3)(e) on legal claims and requirements to evidence 'reasonable efforts' of age verification and parental responsibility under Article 8(2).

Recommendation: These topics need specific further consultation as regards children together with theme 10.

Theme 10: Processing of Children's Personal Data by Online Services

Article 8: Conditions applicable to child's consent in relation to information society services

Relevant recitals

(38) Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

---

[17] UN Committee on the Rights of the Child General Comment No. 12 (2009) on the right of the child to be heard [para 38] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168066cff8

[18] http://www.bbc.co.uk/news/world-europe-37380704

Recommendation: the age of age verification is lowered on a research evidence based approach. This may mean the age is lowered from sixteen to enable freedom of access and rights to participation, but must not stand alone.
Parents cannot consent on behalf of a child. they merely assume responsibility for a verification method and its effects. There must be safeguards and mechanisms in place that ensure other duties in the regulations are respected for all children of all ages no matter what age is agreed upon under derogation of Article 8. Ongoing discussion is needed here.

Internet Governance – Council of Europe Strategy 2016-2019[19]

"Individuals rely on the Internet for their everyday activities and more and more people have access to online services. ***For many, including children and young people, it is their primary source of information and means of expression. The Internet is therefore an invaluable space for the exercise of fundamental rights such as freedom of expression and information.*** *Moreover, it is necessary to raise awareness of legitimate expectations and restrictions when using Internet services, and how to seek redress and remedies when human rights have been violated. The important role played by the media, both new and traditional, as enablers of access to pluralistic and diverse information should be underlined whilst remaining mindful that it is still possible to filter Internet traffic and interfere with Internet content."*

"There are increasing risks to the human rights of Internet users as it becomes easier to connect or to be connected to the Internet and information and communication technologies (ICTs) using every day (household) devices and objects, for example, cars, often referred to as the "Internet of things". Digital tracking and surveillance, ***the collection of personal data, including sensitive data related to health, for the purposes of profiling pose a threat to privacy and the general enjoyment of human rights including freedom of expression and access to information****. Anonymity and encryption tools can help Internet users protect themselves against these threats although respecting their will not to disclose their identities should not prevent member States from taking measures and co-operating in order to trace those responsible for criminal acts."*

Case study|: Questions that need further consideration

If GDPR is not to establish a giant data capture of children and their parents' data including relationship and potential financial status, set up for future commercial capture from the day one that they qualify as "old enough" in Article 8, then derogations must ensure the focus is to verify right to access, not capture personal data, to protect privacy.

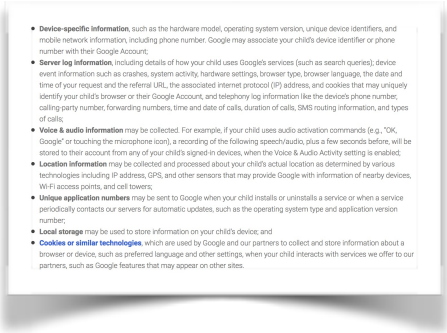
As an example what to avoid, the Google Family Link[20] (beta US only at this time) requires a child's detailed personal data before the Google service will be offered to a child under 13. There is no alternative offered. This means that they develop a database of named 'potential future customer base' with the right "consented to" during sign-up to contact the child as they approach the boundary to inform them that they can now break free from the parental link and oversight.

The risk of verification through signing in via platforms such as Google and Facebook also means the potential expansion of data *capture* by the platforms, which would not have been otherwise necessary using an otherwise independent and unconnected third party website.

Google Family Link (Beta US) for example, captures a significant amount of hidden personal and behaviours data:

"For example, when you create a Google Account for your child, we'll ask for personal information about them, like their first and last name, email address, and birthdate."

Further, "*Information we get from your child's use of our services. We automatically collect and store certain information about the services your child uses and how your child uses them, like when your child saves a picture in Google Photos, enters a query in Google Search, creates a document in Google Drive, talks to the Google Assistant, or watches a video in YouTube Kids."*



- **Device-specific information**, such as the hardware model, operating system version, unique device identifiers, and mobile network information, including phone number. Google may associate your child's device identifier or phone number with their Google Account;
- **Server log information**, including details of how your child uses Google's services (such as search queries); device event information such as crashes, system activity, hardware settings, browser type, browser language, the date and time of your request and the referral URL, the associated internet protocol (IP) address, and cookies that may uniquely identify your child's browser or their Google Account, and telephony log information like the device's phone number, calling-party number, forwarding numbers, time and date of calls, duration of calls, SMS routing information, and types of calls;
- **Voice & audio information** may be collected. For example, if your child uses audio activation commands (e.g., "OK, Google" or touching the microphone icon), a recording of the following speech/audio, plus a few seconds before, will be stored to their account from any of your child's signed-in devices, when the Voice & Audio Activity setting is enabled;
- **Location information** may be collected and processed about your child's actual location as determined by various technologies including IP address, GPS, and other sensors that may provide Google with information of nearby devices, Wi-Fi access points, and cell towers;
- **Unique application numbers** may be sent to Google when your child installs or uninstalls a service or when a service periodically contacts our servers for automatic updates, such as the operating system type and application version number;
- **Local storage** may be used to store information on your child's device; and
- **Cookies or similar technologies**, which are used by Google and our partners to collect and store information about a browser or device, such as preferred language and other settings, when your child interacts with services we offer to our partners, such as Google features that may appear on other sites.

What are the aims of the age verification and what is consent *to"?

In the example given Google and other commercial site providers do not make clear what is consented to capture and how it may be used unless the subject understands how the Internet and their mobile device interact for example.

[19] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ad2a8

[20] https://families.google.com/familylink The Google Family Link app (beta US only at this time (April 2017))

Further, in public interest and/or state actors' research: The ethics of data science are applied patchily at best in government, and inconsistently in academic expectations in for example social media and personal data, or state databases.

"It will no longer be possible to assume that secondary data use is ethically unproblematic."

[Data Horizons: New forms of Data for Social Research, Elliot, M., Purdam, K., Mackey, E., School of Social Sciences, The University Of Manchester, 2013.][21]

Purposes of data collection must be clear and specific, reiterated by the Supreme Court ruling in the Named Persons case on the failure of broad unspecified purposes for data sharing about young people, "The Christian Institute and others (Appellants) v The Lord Advocate (Respondent) (Scotland)" in June 2016, Universal Declaration of Human Rights, the UN Convention on the Rights of the Child, the Charter of Fundamental Rights, and GDPR requirements.

For research purposes exemptions apply, however they cannot be all encompassing, and a nuanced approach is suggested in Article 9 (j) proportionate to the aim pursued, and respect the essence of the right to data protection, and safeguard the interests of the data subject. Can identifiable data be stored and passed to third parties indefinitely at all? "Collect once, use many times" has become the UK mantra in many areas of public service. However GDPR reiterates the Principle 2 of the existing DPA law, the purposes of collection must be explicit and limited at the time of collection.

This is particularly important for children, for whom lifetime of uses may be entirely different in future as technologies and policy changes, as well as their own personal choices and beliefs which may be different from those of their parents - often parents who have taken "consent" choices on their behalf.

Research uses may be made of data using other versions of data: anonymous or synthetic. Today's solutions fail citizens' privacy rights, and to meet the spirit and letter of the GDPR changed processes must aim to deliver alternative solutions. These aspirational goals should be championed by public authorities, not worked around.

The UK Digital Economy Act and Age Verification, and The Digital Strategy and IoT

The guidance [22] on the age verification aspects in the Digital Economy Bill /Act Part 3 is particular to pornography. However, as regards privacy, the detrimental aspects will be similar for any purpose and any data subject, if personal data is captured to perform this task in practice. How this will be done in practice, is important if the aims of the UK Digital Strategy are to be met, and public policy and practice fit for citizens' protection in 'the Internet of Things'.

The same focus must be given to age verification and children's rights to privacy and particular protections, to assure children and parents' privacy and specifically provide method of verification, rather than identification of the individuals and the identifying relationship between child as data subject and a parent as their consent provider. The risks means a reduced data protection, rather than any improvement. *The* Digital Economy Act Guidance states:

"There are various ways to age verify online and the industry is developing at pace. Providers are innovating and providing choice to consumers. The Regulator will not be required to approve individual age verification solutions.

"The process of age verifying for adults should be concerned only with the need to establish that the user is aged 18 or above, rather than seeking to identify the user. The privacy of adult users of pornographic sites should be maintained and the potential for fraud or misuse of personal data should be safeguarded."

"To achieve this, the age verification Regulator should work with the ICO and the Regulator's guidance should include: age verification services and online pornography providers should take a privacy by design approach as recommended by the ICO"; and that *"age verification services and online pornography providers should have regard to the ICO's guidance on (among other things) data minimisation, privacy by design and security."*
Neither The Digital Economy Bill nor the Digital Strategy address these rights and security issues, particularly when posed by the Internet of Things with any meaningful effect. In fact, the chapter Internet of Things and Smart Infrastructure [9/19] singularly miss out anything on security and safety:

"We want the UK to remain an international leader in R&D and adoption of the Internet of Things (IoT). We are funding research and innovation through the three year, £30 million IoT UK Programme."

There was more detail in the 2014 Blackett Review on the Internet of Things (IoT)[23]. This is highly relevant to children.

---

[21] http://hummedia.manchester.ac.uk/institutes/cmist/archive-publications/reports/2013-05-Data_Horizons_Report.pdf accessed 11.04.2017

[22] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/600733/Draft_Guidance_to_the_Age_Verification_Regulator_March_2017__1_.pdf Para 6 (p6 of 13)

[23] https://www.gov.uk/government/publications/internet-of-things-blackett-review

The internet-connected toys 'My Friend Cayla' and 'i-Que' fail when it comes to safeguarding basic consumer rights, security, and privacy. Both toys are sold widely in the EU. The UK government despite our recommendations made in the interests of child safety, has taken no action on this to date. *"If it's not scary enough for the public to think that their sex secrets and devices are hackable, perhaps it will kill public trust in connected devices more when they find strangers talking to their children through a baby monitor or toy." [BEUC campaign report on #Toyfail]*

Recommendation: greater consideration must be given to children, to protect the identity and privacy of their data to limit the potential for fraud or misuse of personal data from a child, which may have lifetime consequences than has been afforded to adults in the Digital Economy Act.

UK Consultation Themes of specific interest as regards the rights of the child and GDPR which merit specific further attention regards the rights of the child

i. Theme 3: Demonstrating Compliance
ii. Theme 5: Archiving and Research
iii. Theme 6: Third country transfers
iv. Theme 7: Sensitive personal data and exceptions
v. Theme 9: Rights and Remedies (with reference to Right to Erasure)
vi. Theme 10: Processing of Children's Personal Data by Online Services
vii. Theme 12: Processing of Data
viii. Theme 13: Restructions

Which elements of GDPR affect children specifically or most? These merit a stand alone consultation.

- Article 6: lawfulness and legitimate interests and the interests of children
- Article 7: right to withdraw consent at any time (for consent based data uses)
- Article 8: parental consent
- Article 12: transparent information provision
- Article 17: right to erasure (sometimes conflated in Right to be Forgotten) and correction
- Article 25: privacy by design
- Article 35: data protection impact assessment
- Article 40: codes of conduct
- Article 57: DPAs awareness
- Recital 38: specific protection
- Recital 58: transparent information
- Recital 65: right to erasure
- Recital 71: profiling (relevant for Progress 8 school attainment forecasting)
- Recital 75 : the risk to the rights and freedoms of natural /vulnerable persons

---

About defenddigitalme

Defenddigitalme is a volunteer non-profit campaign group for children's privacy rights formed in 2015 in response to concerns from parents and privacy advocates about increasingly invasive uses of children's personal data in schools. The campaign asks the Department for Education (DfE) to change their policies and practices to protect 20 million children's identifiable personal and confidential data in the National Pupil Database (NPD):

- stop giving out identifiable personal data to commercial third parties and press without consent
- start telling school staff, pupils, and parents what DfE does with individuals' personal data
- be transparent about policy and practice

For more information see: http://defenddigitalme.com/