children's charities' coalition on internet safety
10, Great Queen Street, London WC2B 5DG

15th May, 2017.

Elizabeth Denham
Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Dear Ms Denham,

An open letter – the GDPR and children

We appreciate it is quite late in the day but hope it is still not too late to draw a number of matters to your attention concerning the implementation of the GDPR, as it will affect children. These are set out below.

We are writing in part because, while we had understood there would be a specific consultation about the position of children, as of now we have heard nothing concrete about when it will take place or in what form. And time is ticking by. Our open letter indicates a number of the issues we are likely to raise at or during any consultation that may yet happen.

We look forward to receiving your comments and are ready to assist if we can.

Yours sincerely,

Secretary

www.chis.org.uk
chisgb@outlook.com

The GDPR: a new order approaches

1. The General Data Protection Regulation (GDPR) comes into force across the EU in May, 2018.

2. It will have a substantial impact on the way in which adult citizens' rights to data privacy are protected and enjoyed. However, at its core, it is possible to see the GDPR as an evolution of a pre-existing set of ideas which, as a result, are reasonably well understood by a body of lawyers, companies, NGOs, and regulators who work in the space. Of course, the GDPR introduces a number of important changes but equally there is much continuity, much that is familiar, at least for today's practitioners.

3. The same cannot be said in relation to the position of children.

The old order departs

4. According to research published by Chatham House and Innocenti ("One in Three: Internet Governance and Children's Rights", 2015), one in three of all human internet users in the world are children. This translates into nearly one in two in parts of the developing world and around one in five in EU Member States. This may well make children the biggest single, identifiable constituency of internet users, and even if that is not literally the case it certainly makes them a very large one.

5. Whatever else we might imagine or want the internet to be it is most definitely a medium for children and families on a large scale. Yet the position of children as data subjects hardly seems to have attracted a commensurate level of attention.

6. The legal regime that is being replaced by the GDPR was established by the Data Protection Directive 1995. In that Directive the words "children" and "age" do not appear at all in respect of anything. Not once. The Directive merely makes a general declaration about the importance of data being processed "fairly" and in that context an individual's age or level of understanding would be relevant factors.

7. Little wider jurisprudence has developed to illuminate how in practice the notion of "fairness" should be interpreted in relation to children although we are aware that the Office of the Information Commissioner (ICO) or its predecessor did issue advice and undertake several enforcement actions.

8. The Article 29 Working Party last looked substantively at an issue concerning children in 2009. This concerned schools' use of children's data (though in 2010 there was a reference to a 2003 code on direct marketing).

9. By contrast, recognising the number of young users has grown enormously since 1995 the GDPR speaks about age under three different headings:

a. It establishes an age below which service providers must always obtain verifiable parental consent as a condition of a child being allowed to use or join their site or service. As we shall see this may vary from Member State to Member State and has yet to be determined in the UK.

b. A corollary of that first age level is that the GDPR also establishes an age at which a young person may decide for themselves whether or not to use or join an online service without the service provider having to obtain any form of consent from anyone else. This age might be called "the age of digital consent" or something similar. It follows that this could vary from country to country and therefore this too has yet to be determined for the UK.

c. It describes a general class of "children". As we shall see, these may be supposed to encompass all persons under the age of 18. This will not vary between jurisdictions within the EU.

A de facto age standard emerged

10. Having said that under the old order age was never explicitly mentioned, in reality a de facto, single standard based on the age of 13 emerged more or less EU-wide. This happened because of decisions taken by the giant US social media platforms pursuant to a US Federal law, COPPA, 1998.

11. Under COPPA, and irrespective of the country in which they were operating, US businesses which directly addressed themselves to young children – in this case all persons under 13 - had to obtain verifiable parental consent for the child to be able to join or remain a member of their service. Disney is an example of a company where all or many of its online services routinely engage in obtaining parental consent.

12. However, COPPA imposed no obligation on companies to age verify anyone so the major social media platforms that intentionally aimed for older audiences simply drew a line at 13. They said nobody under that age could be a member. This obviated the need for them to engage with the messy and potentially expensive business of age verification or obtaining parental consent but it also led to very high levels of misrepresentation by young people who wanted to *"hang out in the cool places"*. The businesses concerned had actively marketed themselves in ways which were bound to have this effect.

13. The term "more or less EU-wide" referred to above is important. In 2007 Spain decided to be different. They chose 14 as their local minimum. Holland already had a standard of 16, however, in both countries it is understood few enforcement actions have been taken.

14. Nevertheless, it should be noted that today in Google's Terms and Conditions 14 and 16 respectively are stated as the relevant minimum ages

for users in Spain and Holland. Inexplicably Facebook appears only to refer to 13 for everywhere.

All change

15. The GDPR thus marks a radical departure from past practice with regard to children. The Commission's original proposal, published in the draft consultation document issued in 2012 was to recognise and establish in law a single EU-wide age of consent for data. They suggested 13.

16. Essentially this would have entrenched the de facto broader status quo, forcing Spain and Holland (not to mention the UK and possibly others also) to change their rules. However, the proposal was thrown out at the last minute. In its place the final version of the relevant rule, enshrined in Article 8, gave Member States a power to choose any minimum age between 13 and 16. They would do this by way of a "derogation". Absent such a derogation by a given Member State the age will become 16 in that country automatically in May, 2018 when the GDPR as a whole takes effect.

17. During the nearly five-year gestation and public consultation period, for good or ill, 13 had been the only specific proposal on the table. As already noted the decision to abandon this and provide a choice of ages was made at the last possible moment (December, 2015). It was completely unexpected and was made without the benefit of any supporting advice or guidance from privacy practitioners. Neither did the politicians who made the decision seek or obtain any advice from anyone within the child welfare or online child protection communities. This was truly a political decision made with a giant capital "p".

18. At first sight the final version of Article 8 appears to have the potential to complicate the operation of the whole Regulation substantially both at the level of national jurisdictions and in the way it will work transnationally.

19. It is quite clear many Data Protection Authorities (DPAs) and others are struggling to get to grips with the full implications of the "new" Article 8. Some are still smarting from the humiliating way in which the decision was taken, still struggling to work out the many layers of its consequences.

A question of evidence

20. The EU is locked into a path which means Member States, including the UK, must choose within the age range specified in Article 8 before May, 2018 or else accept 16 as the minimum. However, if the right people move swiftly enough it should still be possible for the Commission, the European Data Protection Supervisor (EDPS) or an individual DPA e.g. the ICO, to evaluate whatever research currently exists and initiate new, highly targeted research – to help guide national Parliaments or Governments when they make a decision on derogation.

21. The new research suggested here ought to take account of the contemporary internet and the services used by children. It should have regard to and analyse children's ability to understand the nature of the commercial environments they are moving into when they join or use different services, how their data is collected and processed by those services and how it will or might be used. Above all the new research should also be mindful of children's rights to be consulted on matters affecting them.

22. It is acknowledged that a great many adults have a poor understanding of data privacy matters but that hardly seems a good enough basis for accepting that the same should be true for children. Typically, adults can call on other protective factors.

The matter of grooming

23. Only in Ireland, Malta and Cyprus is the age of consent to sex higher than any of the available options for consent to data transactions.

24. This means that, other than within these three countries, it is possible the age of consent for data purposes could end up being the same as or lower than the age of consent to sex. Potentially, this means anyone who visits or uses a site or service in one of the 25 Member States after May 2018, on the face of it will be entitled to assume everyone they encounter is old enough to engage in sexual activity. Will this not compromise or impact upon the operation of the grooming laws in a most unhelpful way? Is there any way this can be avoided? This is particularly important because, absent an efficient and compulsory age verification regime, if the past is anything to go by there will still be considerable numbers of children on the sites or services who have lied about their and are below the age of consent for both data and sex.

25. Even assuming something could be worked out for the 25 Member States, what are the implications for young people in Ireland, Malta and Cyprus?

26. The only available age limit which avoids a potential complication vis-à-vis the grooming laws is 13 because in no EU Member States is the age of consent to sex as low as 13. If 13 was the single, EU-wide age standard nobody would be able to visit or use any site or service and claim they had any reason to believe the person they were talking to *must* be at or above the age of consent to sex.

27. Any alternative to 13 must be able to demonstrate that it can meet the challenges posed by the grooming laws.

Who is a child under the GDPR?

28. The GDPR does not define who qualifies to be described as a child. However, every EU Member State is a signatory to the UNCRC, and the EU itself recognizes the primacy of Treaties such as the UNCRC. The UNCRC defines a child as someone who is under the age of 18.

29. It would therefore be highly desirable for DPAs and the EDPS at the earliest opportunity to confirm that unless the context specifically provides otherwise wherever the GDPR refers to children it means persons under the age of 18. This is important because, as will be noted below, children may not ordinarily be made the subject of profiling.

The Rule of 18 and the Rule of Whatever

30. The DPAs and the EDPS should further explain and illustrate how, if at all, the "Rule of 18" might interact with the "Rule of 13" or whatever different ages of consent to data are eventually decided upon by Member States under the terms of Article 8.

Mixed environments

31. What thought has been given to the implications of having children on the same site or App at the same time, or at different times for that matter, but in jurisdictions where there are different age limits or other relevant rules? The grooming dimension has already been mentioned but there may be others.

32. This is likely to be more of an issue in those countries where the commonly spoken languages are also widely spoken on an international basis. English would most certainly qualify under this heading.

33. This is also going to be important in border areas where, hitherto, the same standards have been applied in adjacent jurisdictions. In the case of the UK, the age of consent to sex notwithstanding, potential difficulties could arise more generally in Northern Ireland if the Republic of Ireland adopts a different age standard from the UK.

Different security standards

34. Where verifiable parental consent *or* age verification is required what data sources and methods will be used and approved by DPAs? Will attempts be made to harmonise approaches?

35. Is it not likely, as things stand, that different countries will have different levels of security or certainty attaching to their processes?

36. If some countries are able to say they are 99.9% positive they have identified Mrs X as being the parent of Child A and that Child A is above

their country's qualifying age of data consent, and other countries cannot get anywhere close to that, where does this leave us?

Lawful processing

37. Under Article 6 personal data can only be lawfully processed if one of the following conditions have been met:

- The data subject has consented to the data processing
- Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- Processing is necessary for compliance with a legal obligation
- Processing is necessary to protect the vital interests of a data subject or another person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority
- Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party

38. It would be useful to develop examples or use cases to illustrate the kinds of situations where each of the above might occur or apply in respect of children. Some are obvious. Others are not.

Special categories of personal data

39. Article 9 refers to several "special categories of personal data" e.g. data revealing racial or ethnic origin, genetic information, data about political or religious opinions and so on. Ordinarily such data should never be collected or processed. However, the Article goes on to say that if certain conditions are met the data *may* be lawfully collected and processed. How might this work in relation to children? Are there any extra steps or safeguards that need to be taken or put in place? Again, use cases or illustrations would be welcome.

Impact assessments and risk

40. What is the intended scope of Article 35 (impact assessments) insofar as it affects children and how, if at all, will it interact with or influence other parts of the GDPR? For example, if there is a higher risk of harm to a child (as opposed to an adult) from a particular data processing activity will this increase the DPAs' expectations of how the service provider addresses it e.g in relation to age verification or parental consent?

41. Article 36 makes clear that "prior consultation" will be required where there is a "high risk". In respect of children what might constitute a "high risk" and how might it be different from a "high risk" for an adult who is otherwise in an identical position?

42. In terms of identifying the sorts of steps a data controller might be expected to take to mitigate a "high risk" does this not imply that the DPA

concerned has sufficient knowledge and expertise in the area of online child protection? Sufficient, that is, to determine whether or not the data controller has acted correctly or adequately. Do many DPAs have that? Does the ICO? If not, how might such expertise be acquired? How will this happen at EU-wide level in respect of the EDPS?

Awareness raising

43. A similar point arises in connection with Article 57 (1) (b). It makes a specific reference to promoting public awareness of "risks, rules safeguards and rights in relation to processing" and activities of this kind addressed to children get a special mention. Again, this implies the supervisory authority has the necessary knowledge and expertise in that area or that they will acquire it.

Codes of conduct

44. Article 40 anticipates the development of codes of conduct. Mindful of the sort of revelations which have already emerged around Barbie Dolls, Cayla Dolls, VTech computers and so on, one obvious early candidate for such a code would be the toy industry and industries which produce Apps or devices which are commonly used in the home or in proximity to children. Schools and the education sector might be another. What happens if they do not choose to develop a code expeditiously? Can they be directed to prepare one and to consult with interested parties?

Stating an age limit but doing nothing to enforce it

45. If a service provider specifies an age limit but fails to put in place any mechanism to enforce it, could they in effect be creating a high risk of harm because in reality what they are doing is teaching children they can lie about their age with little or no risk of discovery or sanction and yet enjoy an undisturbed benefit from such intentional misrepresentation e.g. by becoming and remaining a member of a social media service?

46. Or must an additional factor be present to turn it into a high risk of harm, thereby justifying a DPA requiring the controller to change its approach?

Stating a term or condition but doing nothing to enforce it

47. In a similar vein if a site declares a particular policy but does not make it clear that they make no effort to police or enforce it, does this not amount to a deceptive practice of some sort? End users may rely on the site's or service's declaration of intent without fully comprehending that in reality it is no more than a wish or an aspiration on the part of the supplier or provider who is intentionally relying on the immunity conferred by the eCommerce Directive to avoid any potential liability.

Profiling

Recital 71 of the GDPR prohibits "solely automated processing, including profiling", in respect of children (referring to para 28-29 above, that is persons under the age of 18) unless certain conditions are met.

48. Are there any "profiling processes" that are not "solely automated" that operate over the internet or within other remote environments? What degree of human intervention would be required for a process to be classified as being "*not solely* automated"? It is not hard to imagine how some businesses will seek to circumvent this rule by introducing trivial measures.

49. If such "*not solely* automated processes" exist presumably they could lawfully be deployed in relation to children even though they produce an identical or very similar result to processes which *are* solely automated?

50. Will being exposed to commercial or other forms of advertising be considered a "significant or legal effect"? If so how will this impact on social media platforms or services which are principally or wholly financed via advertising? If the question is to be determined advert by advert it will lead to great uncertainty and unpredictability.

51. Under what circumstance could a child lawfully be exposed to advertisements or other forms of commercial offerings or inducements which might arrive on their screen, *other than by profiling?*

Consents

52. What happens when the GDPR comes into force? Are all previously obtained consents vitiated? This question is raised against a background of knowing there has been a high degree of inaccuracy in previously obtained consents, at least in respect of age levels.

53. A single consent cannot be used for multiple purposes. But at the moment when someone joins, for example, Facebook or YouTube, they are potentially engaging with a number of different types of activity, each of which can generate data that is processed. That being the case how might this matter be addressed when the GDPR comes into force?

54. In the case of Apps or devices which are plainly intended for younger children and which may typically be accessed for the first time via a small screen will it not be the case that more will need to be done to obtain proper consent e.g. by deploying pictograms, cartoons and highly accessible language?

55. Might there be a specific prohibition or limitation on selling devices or Apps for use by children where it is either impossible or very difficult to withdraw or modify consent after the initial setup? Or at any rate could

there be a different and higher set of expectations with Apps or devices of this kind?

56. Where a parent has undertaken the initial sign up process how will authorities ensure a child is able subsequently to withdraw or modify such consent?

57. Might there be a specific prohibition or limitation on selling devices or Apps to children or to be used in connection with children (e.g. baby monitors) where it is either impossible or very difficult for the security settings to be changed, modified or updated?

Medical records, medical matters and the *Gillick Principles*

58. Increasingly patients are being given access to their doctor, other health services and various health records pertaining to themselves via online mechanisms. There may be a commercial or at any rate a monetary dimension associated with some of these services.

59. Are there any special or different considerations which might apply to online access where the records concern a child? Must the holder of the records e.g. the doctor, hospital or pharmacy always obtain parental consent before granting access to the records or systems to a child? Must the parent also be given identical access rights to the child?

60. How will the *Gillick Principles* apply in the new regime? Have the Principles been modified to *any* degree by the introduction of fixed age limits in respect of a young person's ability to engage in data transactions without the requirement to obtain parental consent? The exemption given to "preventive or counselling services" referred to in Recital 38 might not fit all of the circumstances pertaining to records of this type.

61. Could a parent unilaterally modify or withdraw consent in respect of one of their children in relation to the matters discussed here?

Urgent attention is needed

62. There needs to be an EU-wide discussion on these matters. This discussion ought to involve substantial representation from DPAs, the EDPS, the Commission, other privacy practitioners and online child rights experts.

63. How and when might such a discussion be organized? Why has the Article 29 Working Party shown no interest in addressing the position of children under the GDPR, despite repeated requests for them to organize a FabLab or similar on the topic?

Everybody needs help

64. In light of the above there is a strong public interest in children's organizations and other specialised interlocutors concerned with children's

rights to be given the necessary resources to enable them to engage professional data protection lawyers to act as advisers as they seek to chart a path through these unexplored waters. Relying on pro bono assistance or the good offices of academics is not a substitute for professional representation.

---ooo---