Snap Inc.

Response to the Irish Data Protection Commissioner Public Consultation on the Processing of Children's Personal Data and the Rights of Children as Data Subjects under the GDPR

April 5, 2019

Snap Inc.

Introduction

Snap Inc. ("Snap") is responding to this consultation because we believe giving people the power to engage safely, creatively, and positively is critical to their online experience. We encourage parents and teens to have regular conversations about appropriate use of Snapchat and other platforms.

A critical element of this online experience is privacy. That's why at Snap, we make privacy a priority. We know trust is earned every time Snapchat or any of our other products are used.

When we refer to 'children' in this response, we are not referring to children under 13, but are referring to 13-15 year olds (i.e. the minimum age to use the platform, and the maximum age for parental consent in some EU jurisdictions).

For any specific questions on Safety on Snapchat or Privacy at Snap, we refer to our Safety Center[1] and Privacy Center.[2]

Sincerely,

[redacted]

April 5, 2019

[1] https://www.snap.com/en-US/safety/safety-center/
[2] https://www.snap.com/en-US/privacy/privacy-center/

Snap Inc.

I. Children as data subjects and the exercise of their data protection rights

(A) Transparency and the right to be informed about the use of personal data (Articles 12-14 GDPR)

The GDPR requires that individuals must be given certain key pieces of information about the use of their personal data by an organisation (the obligation on an organisation to give this information is known as transparency) and that this information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. This is stated to be particularly important where such information is being provided to children. The transparency information that must be provided where an organisation is processing an individual's personal data includes the identity and contact details of the organisation who is collecting or using the personal data, the purposes and the justification (known as legal basis) for collecting or using the personal data, who the personal data is being shared with, how long it will be kept for, and what the individual's data protection rights are.

1. What methods could organisations who collect and use children's personal data employ to easily convey this transparency information to children?

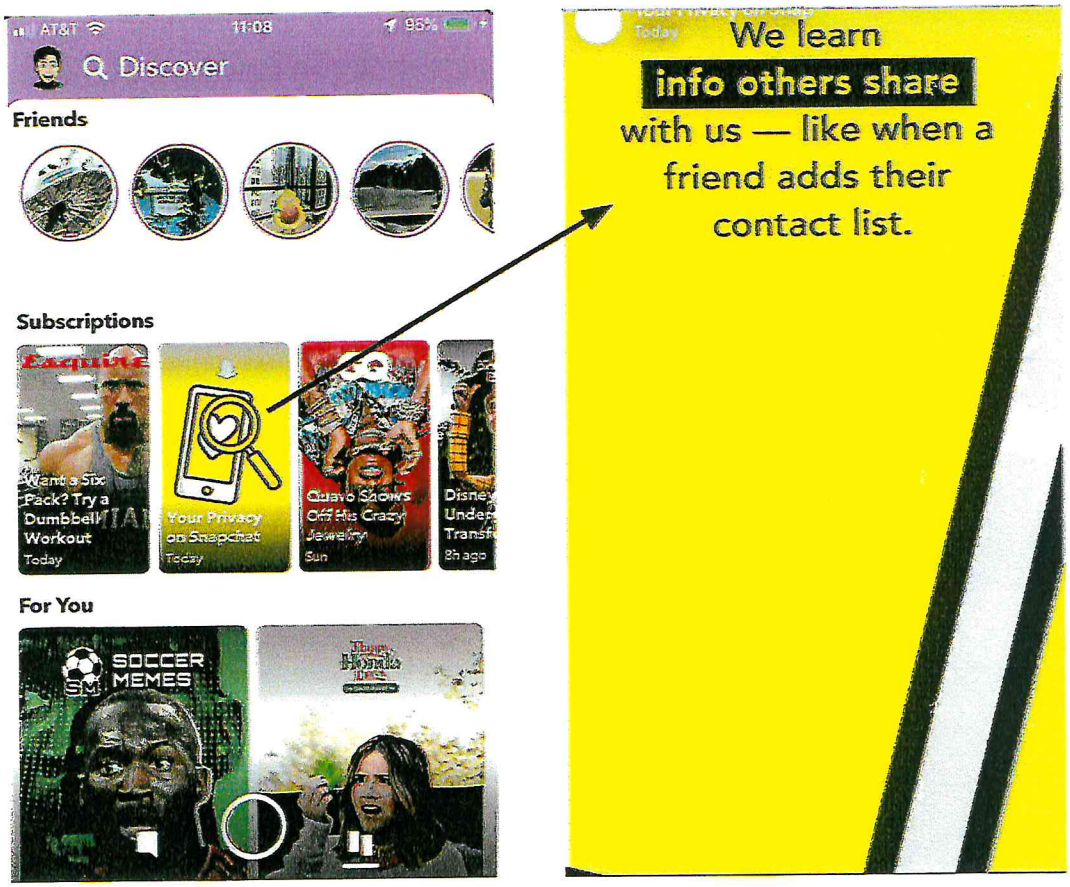
Organisations should focus on integrating transparency in plain language and native to the organisation's platform.

For example, at Snap we created a privacy video to inform users how Snap uses data. This video was displayed in Discover on 25 May 2018, and is still available to users online via our support center.[3] A screenshot of this video is included on the next page.

This video was not just aimed at children, but provides a clear and easy to understand message to all users. Another way Snap applies transparency is through images, icons, summaries and just-in-time notices. At Snap we believe this is a far more effective way of informing users than including everything in a lengthy privacy policy.

[3] See for example, Your Privacy at Snapchat, Explained video: https://support.snapchat.com/en-US/article/snapchat-privacy-explained This video was displayed in the user's discover feed on 25 May 2018, and Snap has resurfaced the video a couple of times as a reminder.

Snap Inc.



2. What approach should be used by organisations whose products or services are aimed at both adults and children? For example, should two separate sets of transparency information be provided that are each tailored according to the relevant audience?

As detailed in the response to Q.1, organisations should not have separate sets for adults and children. Instead, organisations should draft for simplicity and offer layered information through the use of videos, in-app notifications, summaries and icons.

(B) Right of access (Article 15 GDPR)

The right of access is one of the most important data protection rights because it allows individuals to find out whether their personal data is being held by a specific organisation and to obtain a copy of their personal data. Like all other data protection rights, the GDPR does not say when, or in what circumstances, a parent or guardian can make an access request for their child's personal data, or when or in what circumstances a child can make their own access request for their personal data.

3. At what age or in what circumstances should a child be able to make an access request to an organisation and receive a copy of their personal data? Is age the only relevant factor and if not, what other factors should be taken into consideration?

Snap contributed to the Centre for Information Policy ("CIPL") White Paper Implementation in Respect of Children's Data and Consent ("White Paper"), and refers to the CIPL position on access requests:[4]

"CIPL takes the view that the question turns on competence and whether the child has the ability to understand the consequences of exercising his or her rights. Questions of competence are issues of Member State law. The ICO notes in relation to subject access requests that "[i]n Scotland, the law presumes that a child aged 12 years or more has the capacity to make a subject access request. The presumption does not apply in England and Wales or in Northern Ireland, but it does indicate an approach that will be reasonable in many cases".[5]

If a child is deemed not to be competent to exercise his or her own rights then the parent should be permitted to exercise their rights for them, provided this is done in the child's best interest. In the case of a dispute between a child and a parent in the exercise of their rights, consideration should be given to the child's wishes. Article 24 of the EU Charter of Fundamental Rights[6] *states that children may express their views freely and that such views shall be taken into consideration on matters which concern them in accordance with their age and maturity. The Charter further notes that in all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration."*[7]

[4] White Paper, GDPR Implementation In Respect of Children's Data and Consent Centre for Information Policy Leadership, available via: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_gdpr_implementation_in_respect_of_children_data_and_consent.pdf

[5] UK ICO, Subject Access Request, https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/subject-access-request

[6] Article 24 of the Charter of Fundamental Rights of the European Union states that "*[c]hildren shall have the right to such protection and care as is necessary for their wellbeing. They may express their views freely. Such views shall be taken into consideration on matters which concern them in accordance with their age and maturity. In all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration*", Official Journal of the EU 2007, C 303.

[7] White Paper, GDPR Implementation In Respect of Children's Data and Consent Centre for Information Policy Leadership, 6 March 2018, page 26.

4. In what circumstances should a parent be able to make an access request and receive a copy of their child's personal data? Is there an upper age limit after which a parent should not be able to make an access request for their child's personal data? Are there circumstances where both the parent and child should have to jointly make an access request for the child's personal data?

See response to Q.3.

5. How should the balance be struck between a parent's right to protect the best interests of their child and the child's right to privacy when organisations are dealing with access requests for the child's personal data?

In addition to our response to Q.3, organisations should take the age of the child into consideration. If the service relies on parental consent, organisations could require that a request for data is filed by both the child and parent. If the service does not rely on parental consent, the child's privacy rights should prevail. Unless the parent can demonstrate that a request for data is in the vital interests of the child, for example in the event of harassment or bullying.

Snap is committed to providing a safe, fun environment for creativity and expression. To inform users, parents and teachers, Snap has created a Safety Center.[8] Snap also maintains a Safety Advisory Board. This is an external group of five outside safety and privacy experts that provide us with strategic advice and help shape Snap's approach to important safety issues. These board members are on the front lines of privacy and safety policy issues everyday -- speaking, writing, and advising -- and their enhanced understanding of Snap will help us in the future. For these reasons and so many more, Snap recently organized a full-day workshop for them at Snap's headquarters.

(C) Right to erasure ("Right to be forgotten" – Article 17 GDPR)

Individuals have the right to have their personal data erased, without undue delay, by an organisation if certain grounds apply. This includes where personal data was collected by an online service provider in circumstances where the individual now making the erasure request originally gave their consent to have their personal data used or collected when they were a child. The GDPR says that where this has happened, an individual should be able to request that their personal data be erased because, having been a child when they consented to the collection and use of their personal data, they may not have fully understood the risks of doing so.

[8] Snap Safety Center: https://www.snap.com/en-US/safety/safety-center/.

6. At what age or in what circumstances should a child be able to make an erasure request to an organisation and have their personal data erased? Is age the only relevant factor and if not, what other factors should be taken into consideration?

At Snapchat data deletion is our default. Snapchat aims to capture the feeling of hanging out with friends in person — that's why Snaps and Chats are deleted from our servers once they're opened or expired.

We don't believe companies should maintain a permanent record of all the interactions between users. This is especially the case for children. They should not be haunted by their digital past.[9] Children today grow up in the digital age, where every moment of their lives can be captured and shared. Parents, older siblings and others post pictures of kids on their social media profiles with the best intentions, but with little consideration for the privacy rights of these children. It is not uncommon for these social media profiles to be public, for all the world to see, which raises concerns about scraping and potential misuse of content. Children should be protected, informed and empowered to exercise their privacy rights. An effective way to do this is to allow children to request the deletion of their data, which should include data that was shared about them by others, such as parents.

In addition, Snap refers to the CIPL position on erasure as detailed in the above referenced White Paper:

"(...)Taking Article 17 (the right of erasure) as an example, under the above logic, a child would be able to exercise this right if they understood the consequences of doing so and had the competence to exercise the right as determined by Member State law. Recital 65 supports this notion by stating that "the right [of erasure] is relevant in particular where the data subject...is not fully aware of the risks involved by the processing...[and] the data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child". This seems to imply that where a data subject is fully aware of the risks as a child (i.e. has the competence to exercise their rights) they should be able to exercise their right of erasure.

Article 17(1) clarifies that a data subject (which includes a child) can exercise his or her right of erasure where one of a number of grounds apply. Of particular relevance are Articles 17(1)(b) and 17(1)(f). Article 17(1)(b) states that a data subject can exercise the right of erasure where the data subject withdraws consent. For processing outside the scope of Article 8, a child would be able to withdraw consent and thus exercise the right of erasure if they are deemed competent to do so. Article 17(1)(f) clarifies that the data subject can exercise the right where personal data have been collected in relation to the offer of information society services referred to in Article 8(1). Though a child under the threshold age may not be able to withdraw

[9] See for example the Fast Company article 'I'm 14, and I quit social media after discovering what was posted about me' available at: https://www.fastcompany.com/90315706/kids-parents-social-media-sharing

consent in this scenario, as they had not provided it in the first instance, Article 17(1)(f) clearly provides for the data subject (i.e. the child) to exercise their right of erasure where the data has been collected in relation to Article 8(1). It is important to remember that just because the HPR gives consent or authorises the child to give consent to the data processing under Article 8(1), the HPR is not the data subject, the child is. CIPL considers that controllers should be able to assess the age at which a child is competent to exercise his or her own rights in accordance with the law of the relevant Member State unless otherwise notified that a child does not have competence."[10]

7. In what circumstances should a parent be able to make an erasure request on behalf of their child and have their child's personal data erased? Is there an upper age limit after which a parent should not be able to make an erasure request for their child's personal data? Are there circumstances where both the parent and child should have to jointly make an erasure request?

In addition to the response to Q.6, a parent's request for erasure on behalf of their child (13 and older) should preferably be filed jointly by the child and parent. A request for erasure could result in the loss of data created by the child, e.g. avatars, images, photos etc. that have value to the child. If a service does not rely on parental consent, parents should not be able to file a request for erasure on behalf of their child, unless the parents are able to demonstrate that this is in the vital interests of the child.

[10] White Paper, GDPR Implementation In Respect of Children's Data and Consent Centre for Information Policy Leadership, 6 March 2018, pages 26-27.

II. Safeguards (A) Age verification (Article 8 GDPR)

In Ireland, children below the age of 16 (the "age of digital consent") cannot give consent to online service providers to process their personal data. If consent to process personal data is requested by the online service provider in order for the child to access the service, parental consent must be given. This means that consent must be given by the person who holds parental responsibility for the child. However, the GDPR requires that the online service provider must make "reasonable efforts" to verify that consent is given by the holder of parental responsibility "taking into consideration available technology".

8. If an online service provider is relying on consent as their legal basis (justification) for processing children's personal data, what methods could/should be used to verify that a child is 16 or over in order that the child is granted access to the online service without the need for parental consent?

One of the core principles of data protection law is data minimisation. Organisations should avoid asking for more information than necessary to verify the age of the user. For example, companies should refrain from requesting copies of passports or ID cards. Age gating is a good practice, and if services are directed at children - companies can consider implementing a parental consent mechanism.

See also CIPL White Paper guidance on this point:

"(...) CIPL is of the view that the risk assessment should be designed to determine whether the ISS is offered directly to a child as discussed above and not to determine whether it is necessary to collect age-related information.

Where an appropriate risk assessment has been carried out and indicates that an ISS is offered directly to a child, then any processing of children's data on the basis of consent can only occur if consent is given or authorised by the HPR. For children who have reached the age of digital consent, there should be a mechanism in place for such children to indicate that they have reached the relevant age threshold and that allows them to proceed with the service without obtaining parental permission. The mechanism should be proportionate to the nature of the site and the service or material which it provides. In certain cases, self-declared age tools may be considered valid. Any data collected by organisations to this effect, and which is not required for evidential purposes and has no other function, should be immediately deleted following verification, to ensure compliance with the principle of data minimisation.

For ISSs that are not directed to a child but which are available to children, organisations should ensure the age threshold contained in the terms of service is communicated upfront in a

clear way to new service users. Additionally, the organisation should take reasonable and proportional measures to enforce the age threshold and where appropriate, put measures in place to prevent or deter underage users from using the service, such as ensuring that any actual knowledge received of an underage user engaging with the service is appropriately acted upon.

In summary, a risk based-test should be developed to determine whether an ISS is offered directly to a child, taking into account whether the ISS offering is made intentionally attractive to children. The development of such a test may usefully engage a multi-stakeholder process. It should be recognised that appropriate practices may continue to be developed with an open approach to innovative developments."[11]

9. (a) What methods could/should online service providers use to ensure that the person providing consent in these circumstances is actually the holder of parental responsibility over the child?

Organisations could look at COPPA best practices developed in the US. For example, requiring a consent form to be printed and returned via mail, fax or scanned; require a credit card, or other online payment system to notify the primary account holder, require the parent to call or video conference with the organisation or check government issued identification.

(b) What constitutes a "reasonable effort" made by organisations to verify such consent is being given by a person who is actually the holder of parental responsibility over the child? How should "reasonable efforts" be measured in this regard?

Reasonable efforts should be measured in light of the services that the child can access and the type of data the organisation will process. For example, if the child provides medical or other sensitive data, the reasonable efforts an organisation should take are higher than when a child is accessing a service that handles less sensitive data.

Generally speaking, the age-verification of minors is complex and there are several legal and technical challenges that are still to be resolved. For example, age verification would require the collection and retention of documents such as a copy of passports, driving licences or other documents and the ICO has said it has "significant concerns" that this data would be vulnerable to misuse and/or attractive to disreputable third parties. A solution would be a government approved UK database or ID system for minors, but this currently doesn't exist.

[11] White Paper, GDPR Implementation In Respect of Children's Data and Consent Centre for Information Policy Leadership, 6 March 2018, page 15.

Snap Inc.

There are millions of apps with a need for robust age verification be that messaging, content, social media, video, gaming or adult content and it seems inefficient to try and manage age verification at this level. However, the alternative the ICO has previously raised is device level verification. Both Apple and Google offer solutions at this level. Family Sharing on iOS includes an Ask to Buy feature, which is on by default for children under the age of 13 and allows parents to control which apps their children download. Similarly, Family Link on Android allows parents to manage apps, keep an eye on screen time and set a bedtime for their child's device.

10. Prior to 25 May 2018, there was no law setting the age of digital consent in Ireland, but many online service providers required users to be at least 13. If an online service provider now is aware that an existing user of their service is under 16, should the user be locked out of the service until they reach 16?

We refer to the CIPL guidance on this point:

"Organisations impacted by Article 8 GDPR are facing a practical issue of how to deal with existing ISSs users who may be considered a child from 25 May 2018 under the GDPR and applicable Member State law. Should the controllers obtain consent from the HPR where required, while in the meantime freezing the account and suspending the service until that consent is lawfully obtained? This does not seem practicable and will deprive users of services that they may have been using for years. Individuals would be faced with the significant burden and potential annoyance of having to obtain parental authorisation to re-consent to processing to which they had previously consented and that has not changed.

CIPL suggests that organisations could rely on legitimate interest following an appropriate notification and balancing test to continue services for those who will be under the age of consent after 25 May 2018. Changing legal basis of processing is possible provided there exists a valid alternative legal basis, the GDPR requirements on notice and transparency are fulfilled and the requirements of the alternative legal basis are met. Legitimate interest in this respect may include not only data controllers' interests but also those of third parties (such as content right holders). When carrying out the balancing test, the child's interest in continued use of the service should also be considered. This ensures minimal disruption to existing users while ensuring that new processing of data – whether for new users under the age of digital consent or for material changes to processing for existing users – for ISSs offered directly to a child based on consent will comply with Article 8 GDPR."[12]

[12] White Paper, GDPR Implementation In Respect of Children's Data and Consent Centre for Information Policy Leadership, 6 March 2018, page 27-28.

(B) Online service providers and different national ages of digital consent in the EU (Article 8 GDPR)

Many online service providers offer services in multiple EU countries where there are different ages of digital consent. For example, while the age of digital consent in Ireland is 16, in Spain it is 13, and in Austria it is 14.

11. How should such online service providers ensure they comply with different ages of digital consent in different Member States?

The lack of harmonisation on this point is a great burden for users, parents and organisations. As a best practice, companies could look at the country of signup or the IP address of the user, and age gate on a country-by-country basis. For example, a user registered in Ireland who is 14 may require parental consent to use certain services, whereas a user in Spain of the same age would be able to use the service without parental consent.

III. Profiling and marketing activities concerning children (Articles 21-22 GDPR)

Profiling is a way of using someone's personal data to predict or analyse characteristics about that person, such as services they will be interested in, their likes or dislikes, preferences, views or opinions, or their behaviour, amongst other things. For example, organisations may collect information from their customers or users to try to predict other services or products they might be interested in. A user profile can be a really valuable tool in revenue terms for an organisation because the detailed information on an individual contained in a profile can help the organisation to tailor information, advertisements and marketing materials, amongst other things, precisely to a person's interests, needs or individual views. For example, if an individual often clicks on posts online about a specific singer or "likes" pictures of clothes from a particular shop, they may start to see ads for tickets to that singer's concert or similar artists' concerts popping up on their social media feed, or ads might start appearing telling them that there is a sale on in that particular shop or similar shops. That is because online operators are constantly collecting and frequently sharing with each other this type of information about users and adding it to the profile being built about them. In this way, the user's profile then becomes the basis upon which specific advertising and marketing materials are selected to target that user. The GDPR does not impose an outright prohibition on organisations marketing or advertising to children, but it does say that they should apply specific protections for children when marketing to them or creating user profiles. Additionally, collective guidance issued by the EU's data protection authorities (European Data Protection Board ("EDPB")) advises that, because children are more vulnerable, organisations should, in general, refrain from creating individual profiles on children for marketing purposes. All individuals (including children) have the right to object at any time to their data being processed for direct marketing purposes.

12. In the case of marketing to a child, what factors should be taken into consideration when balancing an organisation's own legitimate interests in conducting direct marketing and the interests and rights of a child who is being marketed to?

We refer to the CIPL White Paper guidance on this point:

"The ICO Consultation clarifies that there is no absolute barrier to marketing to children under the GDPR, although it notes guidance and restrictions in other codes and legislation.[13] It makes clear that any marketing must be fair and not exploit the vulnerability of children. Children have the same rights to object to marketing as adults (provided they are competent to exercise such

[13] For example, the UK Code of Non-Broadcast Advertising and direct and promotional marketing (CAP code), https://www.asa.org.uk/codes-and-rulings/advertising-codes/non-broadcast-code.html Similar codes have been created by other Member States (e.g. 7th Edition of the Code of Standards for Advertising and Marketing Communications in Ireland, http://www.asai.ie/asaicode/ and the French ARPP on the rules of ethics applied to advertising in France, https://www.arpp.org/nous-consulter/regles/regles-de-deontologie/).

rights by virtue of Member State laws on competence) and these must be clearly explained in a way that is accessible to the child. The ICO also notes that it may be inappropriate to collect and use profiles of children for marketing purposes. Other European laws on marketing practices are also relevant with respect to children, for example, Directive 2005/29/EC on Unfair Commercial Practices which lists "including in an advertisement a direct exhortation to children to buy advertised products or persuade their parents or other adults to buy advertised products for them" as an aggressive commercial practice.[14]

The GDPR generally accepts that marketing, including profiling, can take place on the basis of legitimate interest, subject to the proper balancing test and safeguards. This indicates that processing personal data for marketing is broadly recognised as being a common and expected activity.

Additionally, codes of conduct under Article 40(2)(g) of the GDPR could be created to provide more certainty with regard to marketing practices for children under the GDPR.

In summary, while it depends on a multitude of factors whether a data processing operation implies risks for individuals, processing personal data of children for advertising to them is not sufficient to rate the processing as high risk and there should be no preconceived notion to the contrary. This should be emphasised in any regulator guidance on children's data and the GDPR."[15]

13. Should organisations be prohibited from profiling children for marketing purposes? If so, should this be age-dependent or dependent on other factors? If so, what are these other factors?

We refer to the CIPL guidance:

"The ICO Consultation correctly explains that there are no specific references to children in Article 22 of the GPDR. However, Recital 71 states that generally children should not be subject to a decision that produces a legal effect or similarly significantly affects them that is solely based on automated processing, including profiling.

The WP29 guidelines on automated decision-making note, however, that given the wording of Recital 71 is not reflected in the Article itself, the WP29 does not consider that the Recital represents an absolute prohibition on this type of processing in relation to children. The guidance continues by stating that there may be some circumstances in which it is necessary

[14] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ("Unfair Commercial Practices Directive"), Annex I, point 28, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32005L0029.

[15] White Paper, GDPR Implementation In Respect of Children's Data and Consent Centre for Information Policy Leadership, 6 March 2018, page 21-22.

for controllers to carry out solely automated decision-making, including profiling, with legal or similarly significant effects in relation to children, for example to protect their welfare. The WP29 further provides, in its guidelines, information on what it considers to be an automated decision that produces similarly significant effects on an individual.

The WP29 notes that the decision must have the potential to:

- *Significantly affect the circumstances, behaviour or choices of the individuals concerned;*
- *Have a prolonged or permanent impact on the data subject; or*
- *At its most extreme, lead to the exclusion or discrimination of individuals.*

The WP29 acknowledges that it is difficult to be precise about what would be considered sufficiently significant to meet the threshold, but it puts forward some examples of decisions which could fall under Article 22. These include decisions that affect someone's financial circumstances, affect access to health services, deny employment opportunities or affect access to education. The WP29 also notes that in many typical cases automated decisions to present targeted advertising based on profiling will not have a similarly significant effect on individuals.

The ICO Consultation notes that if Article 22 does apply, the controller is not prohibited from profiling children but should pay careful attention to Recital 71 and to the WP29 guidelines which state that as a rule, controllers should not rely upon the exceptions in Article 22(2) to justify the automated decision. However, this is not an absolute bar and the ICO continues to state that if a controller does rely on one of the Article 22(2) exceptions, the controller must demonstrate there are suitable measures in place to properly protect the interests of the children whose personal data it is processing.

It is important to recall, however, that for an automated decision to produce a similarly significant effect it must rise to the same level as producing a legal effect, which is a high bar and many forms of automated decisions are unlikely to fall under Article 22 of the GDPR. Therefore, it is crucial that Article 22 is interpreted narrowly to ensure that automated decisions not producing legal or similarly significant effects are not mistakenly caught under the scope of Article 22.

The ICO suggests taking into account specific criteria when assessing whether a solely automated decision has a similarly significant effect on a child in the context of behavioral advertising. These include (i) the choice and behaviours the controller seeks to influence, (ii) the way in which these might affect the child and (iii) the child's increased vulnerability to this form of advertising.

While CIPL agrees these are undoubtedly relevant factors, it may be useful to specify that these are examples of the types of factors that should be taken into account, and not an exhaustive

or compulsory list. Retaining flexibility on the criteria that should be taken into account would allow for a more tailored approach."[16]

[16] White Paper, GDPR Implementation In Respect of Children's Data and Consent Centre for Information Policy Leadership, 6 March 2018, page 22-23.

Snap Inc.

IV. Data protection by design and by default (Article 25 GDPR)

The GDPR imposes a new obligation of data protection by design and by default on organisations who process personal data. This means that data protection and privacy protection should be built into a product or service from the very start of the design process (rather than being considered after the development phase) and that the strictest privacy settings should automatically apply to a product or service (rather than the user having to activate them). These obligations are particularly relevant considerations for organisations whose products or services are used by or offered to children.

14. What measures should organisations take to incorporate the principles of data protection by design and by default into the services and products that they offer to children?

Organisations should focus on minimizing data collection, limiting data retention, offer actual control and be transparent with users.

At Snap these elements are encompassed in our privacy principles. These principles are front and center on Snap's Privacy Center.

These principles can be summarized as follows:

> **We communicate honestly and openly**
> When you use Snap products, you share information with us — it's our responsibility to help you understand how that information is used. Our Privacy Policy[17] explains how we collect, use, and share information — you can read the highlights here.[18]
>
> **You choose how to express yourself**
> We believe that privacy is essential to empowering self-expression. That's why you're in control of who you share things with, how you share them, and how long they can be seen.
>
> **We design with privacy in mind**
> New features go through an intense privacy review process — we talk about things, we debate them, and we work hard to build products we're proud of and that we'll want to use.

[17] https://www.snap.com/en-US/privacy/privacy-policy/.
[18] https://www.snap.com/en-US/privacy/your-privacy/.

Snap Inc.

You control your information
You have the right to control your information. That's why we provide easy ways to access and update your information, adjust how much information you share with us, and request that we delete your information — or your account, altogether.

Deletion is our default
Snapchat aims to capture the feeling of hanging out with friends in person — that's why Snaps and Chats are deleted from our servers once they're opened or expired.

15. Do you think products/services that are used by or offered to children should have built-in default privacy settings that vary according to the age and evolving capacities of a child? For example, should there be stricter privacy settings for younger children? How should these variations in the privacy settings be given effect?

Yes. Companies should restrict privacy sensitive features to children. For example, organisations could limit publishing children's content on public versions of their services. Another area where companies should treat children's data differently is in terms of data retention. Short data retention terms significant reduce privacy risks, and prevent organisations from creating a permanent record.

V. General

16. Are there any other particular issues you would like to raise with the DPC in connection with the subject matter of this consultation?

N/A