To:
Children's Consultation
Data Protection Commission
21 Fitzwilliam Square, Dublin 2
Republic of Ireland
childrensconsultation@dataprotection.ie

28 February 2019

RE: Comments on the Consultation: Public Consultation on the Processing of Children's Personal Data and the Rights of Children as Data Subjects under the GDPR

Dear Commissioner,

We write to provide comments on your Public Consultation on the Processing of Children's Personal Data and the Rights of Children as Data Subjects under the GDPR.

By way of context, SuperAwesome is the leading provider of 'kidtech', technology and services used by companies worldwide to enable safe, compliant (COPPA, GDPR) digital engagement with children. We have over 250 customers who use our technology across industries including toy, film, entertainment and video games. From our London headquarters, our team of 140 employees, including more than 40 software engineers, are developing and rolling out Privacy by Design technology focused on the needs of the children's digital media ecosystem globally.

Our technology is used by content owners (websites, apps), brands and agencies to comply with children's data privacy rules and appropriate content standards in each territory. In particular we serve advertisers and publishers who want to deliver advertising without collecting any personal data, and who wish to comply with COPPA in the US and GDPR-K in Europe when it comes to offering services to children.

Our advertising platform is connected to online services (ISSs) that serve an aggregate of 80M children and teenagers across the EU. Every advertisement delivered by our technology is watermarked with our SafeAd logo, which signifies that the ad (1) is not collecting any personal data (including persistent identifiers), and (2) has been reviewed by a human for age appropriateness.

In addition, our KidAware education programme is used extensively by brands and agencies to train their employees in children's data privacy laws and advertising standards - we educated well over 180 UK digital media professionals in 2018.

Finally, we have been actively involved in working with the market and regulators in developing and implementing digital child safety policies, including:

- Being active on the board of Mediasmart, which designs and distributes media literacy materials in UK schools, and is currently developing teaching materials for data privacy awareness.
- Contributing actively to the ASA's revisions to the CAP Code, in particular the April 2017 guidance on labelling and disclosure of native advertising aimed at children.
- Working closely with industry associations such as Toy Industries Europe (TIE), and the British Toy & Hobby Association (BTHA) to educate and advise their members on data privacy compliance.
- Submitting comments to the Working Party 29 consultations on Profiling and Automated Processing, Transparency and Consent, to the ICO's consultation on Children and the GDPR, and to the Australian Competition and Consumer Commission's Digital Platform Inquiry Preliminary Report.
- Regularly speaking at events hosted by the Nordic Privacy Forum, Family Online Safety Institute (FOSI), and the Children's Advertising Review Unit (CARU) about the intersection of law and technology when it comes to children's data privacy.

Our nearly 6 years of experience in building technology platforms for compliance gives us a unique insight into practical, technology-based solutions to the most difficult challenges, including age verification, parental consent, disclosure for kids, and assessing the relative risk of different tracking technologies.

Our attached comments are provided in order to assist businesses to become fully compliant—in both the letter and spirit—with the GDPR when it comes to engaging with children online.

We hereby consent to the publication of personal data contained in this attached document.

Yours sincerely,

[redacted]

SuperAwesome Trading Ltd

SuperAwesome's comments on the DPC's Consultation: Processing of Children's Personal Data and the Rights of Children as Data Subjects Under the GDPR

Our comments address eight areas of the consultation:

1. Verification of children over the age of digital consent
2. Parental responsibility:
    a. Methods of verifying the holder of parental responsibility
    b. Definition of "reasonable efforts" when verifying the holder of parental responsibility
3. Denial of service
4. Compliance with fragmented ages of consent
5. Considering factors for Legitimate Interest for direct marketing
6. Profiling of children for direct marketing
7. Privacy by Design principles when offering services/products to children
8. Privacy settings according to age and evolving capacities of a child

1. **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?**

    Establishing an individual is 16 or over may at first instance appear straightforward since individuals 16 and over are likely to hold identity documents such as a National Insurance Number, national ID, drivers licence, etc. These can be used and matched against available databases to verify age.

    However, data collection and processing for the purpose of age verification should be proportionate to both the context of the processing risk in relation to the online service, as well as the method for carrying out the verification. This has been emphasized by the EDPB by proposing that online services should make a risk-based assessment of the proposed processing when selecting an appropriate age verification mechanism which in turn, "should not lead to excessive data processing."[1]

    Since it is generally difficult to reliably verify age without also verifying identity, the DPC should be cautious of any proposed mechanisms that involve additional detailed collection of any individuals' personal data that is not relative to the data processing risk. We therefore submit that for common data processing activities (such as, for example, email address for password reset, or geolocation data to enable an augmented-reality game), any technique that requires the incremental collection of personal data such as national insurance number or national ID card would constitute as an overly intrusive method of age

[1] Article 29 Working Party, Guidelines On Consent Under Regulation 2016/679 (2018), p. 25

verification. We refer the DPC to *Table 1* in 2(a) which contains further recommendations which we believe would constitute as appropriate age verification methods that respect the data minimization principle.

2. **(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?**

The GDPR's Article 8 introduces the concept of parental verification. While a new concept under European law, the notion is clearly borrowed from the Children's Online Privacy Protection Act (COPPA) in the US. Unlike COPPA which prescribes specific methods for obtaining parental verification,[2] the GDPR is non-prescriptive in this respect.

As such, European regulators have recommended proportional methods to achieve parental verification. The EDPB suggests that organizations take the data processing risk into account[3] and only obtain what is necessary such as basic contact details of the parent or guardian[4] to carry out verification procedures. The ICO in the UK has taken a parallel interpretative approach, indicating that it may be acceptable to use an email declaration or tick box to affirm that an individual holds parental responsibility where there is a low-risk processing activity (e.g. subscribing to a newsletter via a website).[5] Conversely, the ICO suggest that in high-risk scenarios such as unmoderated online communities, more stringent methods of parental verification (e.g use of a third party) may be warranted.[6]

SuperAwesome welcomes this proportionate, risk-based approach and urges the DPC to adopt similar measures. This would enable organizations to minimize the amount of additional data collected for verification purposes, keeping within the data minimization principle. We have provided what we believe to be a practical framework (*see Table 1*) as well as some further examples (*see Figure 1*) below. This has been developed based upon our extensive experience in working with children's online services, and enabling parental consent and verification flows for COPPA compliance.

Table 1 Risk-Based Approach to Verification

Type of data collected	Sensitivity	Examples of sites or apps	Appropriate method to verify user is over age of consent	If not, parental consent required?

[2] Children's Online Privacy Protection Rule, 16 C.F.R., §312.5(2)(b)
[3] See n. 1, p. 26
[4] *Ibid.*
[5] ICO, 'What Are The Rules About An ISS And Consent?' available at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/what-are-the-rules-about-an-iss-and-consent/> accessed 21 February 2019
[6] *Ibid.*

				Appropriate verification method
Sensitive Personal Information (health, ethnicity, tied to a name or ID number, etc)	Very high	Ancestry or healthcare service that stores user profiles with identity information and demographic/ ethnic/health data.	Neutral age gate, plus Database check against national registry, or Copy of photo ID submitted	**Identity-Verified Parental Consent (w/ database)** 1. Parent provides consent 2. Statement by parent that he is the holder of parental responsibility; 3. Parent identity checked against national ID database, or by submitting copy of photo ID
Identifiable personal information, eg full name, address, national ID number; image/video uploads; free text content. Combination of online identifiers and profile information that can be used to identify a natural person	High	Social media app that allows use of real names, connections with strangers, free-text chat rooms Virtual assistant that records voice & stores it in cloud, builds usage profiles.	Double confirmation, eg Neutral age gate, plus Reconfirmation of birth year; or, Two-factor confirmation, eg Neutral age gate plus Confirmation provided by email or text message	**Identity-Verified parental consent (no database)** 1. Parent provides consent 2. Statement by parent that he is the holder of parental responsibility; 3. Identity is confirmed by requesting credit card details and matching them against information provided (no transaction). Credit card information is then immediately deleted.
Technical online identifiers that cannot easily be resolved to a natural person, but are (a) shared with third parties, and/or (b) used for behavioural advertising & profiling, including geo-location Creation of a unique username (not PII)	Medium	Websites that allow behavioral or profile-based advertising. Virtual world, or games app that includes username registration, leaderboards	Double confirmation, eg Neutral age gate, plus Reconfirmation of birth year; or, Two-factor confirmation, eg Neutral age gate plus Confirmation provided by email or text message	**Verified Parental Consent** 1. Parent provides consent; 2. Statement by parent that he is the holder of parental responsibility.
Enabling of notifications (eg, push) City-level geo-location information	Low	Apps that request permission to send push notifications; provide services based on city location (eg transport)	Confirmation that subject is over age of consent, via a simple, neutral age gate	**Direct Notice.** Opt-in, and direct notice sent to parent, stating type and purpose of collection and linking to Privacy Policy. No further verification of parental holder of responsibility

Technical online identifiers used for internal operations purposes only (analytics, contextual advertising, personalisation, security) Country-level geo-location information	Low	Casual games site with no registration, only contextual advertising	Processing on **Legitimate Interest** basis. No age check required.	Processing on **Legitimate Interest** basis. Parental consent not required. n/a
No data collection	None	Corporate website for marketing purposes, no advertising, no trackers	No age check required.	Parental consent not required. n/a

Situational Examples:

Example 1: An educational website which primarily finances itself through advertising.

If advertising is delivered contextually *and* there is no cross-domain tracking, then this should represent a low level of risk to the individual and should not require age verification or parental consent. The publisher (website operator) should have to ensure that all technology and advertising partners are aware of the nature of the site (i.e. it is child-directed) and should further be held responsible for guaranteeing that there is no collection of online identifiers which could be used to profile users. Social media plugins should not be allowed.

Example 2: A mobile social application that enables individuals to chat, connect with friends, and share content with the use of real names.

The use of real names, open text chat, and the ability to connect with strangers makes this a high risk to individuals' privacy. In this scenario, a service should require age verification and/or verified parental consent.

Example 3: A virtual world that allows social interactions between anonymous avatars.

This could represent a low risk situation provided that appropriate measures are in place to prevent disclosure of personal information (e.g. the filtering of potential real names, phone numbers, etc. in unmoderated channels or chat rooms). Therefore, no age verification or parental consent should be required in such a scenario.

Example 4: A voice-based virtual assistant, or Internet-connected toy.

We recognize that this scenario would combine the issue of ePrivacy and GDPR given the electronic communicative nature of connected toys (we do note that the ePrivacy Directive does not necessarily include IoT devices however, we are aware that the future Regulation would). The concern in this instance, is the manner in which voice data may be stored and subsequent analysis and use of that data in the Cloud. Due to these components and the known security risks of connected devices, we would consider this to represent a high risk and should require both age verification and verified parental consent.

If the service provider in this instance, can demonstrate that it is using collected audio files solely for purposes of transcribing a command and immediately deletes the file thereafter for example, we may consider this as a moderate risk, potentially requiring a simple opt-in and direct notice to parents.[7]

Figure 1: Situational examples to assist in giving the DPC further context

2. **(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?**

   We refer the DPC back to our answer in 2(a) and in particular, *Table 1* which outlines what we believe to be reasonable efforts taking into account currently available technology. This question is therefore not dissimilar to 2(a) and would suggest the DPC take a pragmatic, risk-based view as both the EDPB and ICO on the notion of "reasonable effort."

3. **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?**

   Fundamental Rights and Freedoms are applicable to *everyone*, regardless of context. Children therefore enjoy Fundamental Rights just the same as adults under the Charter of Fundamental Rights and Freedoms, the ECHR, as well as the UNCRC.[8] With children increasingly experiencing most aspects of their lives digitally, it has been well recognized

[7] Federal Trade Commission, FTC Provides Additional Guidance on COPPA and Voice Recordings (Oct 2017), available at <https://www.ftc.gov/news-events/press-releases/2017/10/ftc-provides-additional-guidance-coppa-voice-recordings>; we recommend following the best practices as set out by the FTC on virtual digital assistants

[8] Article 1 of the ECHR applies to "everyone" without discrimination and therefore includes children. We have mentioned the Charter here, however we have found that the ECtHR has a wider body of case law as it pertains to privacy rights online, as well as children's rights (see generally, European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Law Relating to the Rights of the Child (2015))

that the Internet plays a crucial role for enabling Rights and Freedoms online.[9] These include rights such as the freedom of expression,[10] freedom of association,[11] and the right to privacy.[12] In addition, the Charter includes the right to data protection,[13] and the UNCRC includes the right to access a diversity of media.[14]

Under the ECHR and UNCRC, some rights—such as freedom of expression,[15] freedom of association[16] and, under the ECHR more specifically, the right to privacy[17]—are not absolute and can therefore be limited in scope and nature. Despite the right to privacy being in essence a protectionist right, the DPC would *not* be justified in allowing or requiring service providers to lock under-16's out of a service. Although the ECHR is not directly binding on any other country except for the one in dispute, the DPC should be aware that the right to privacy has (in various other countries) included the right to establish and develop relationships with other human beings,[18] as well as a general acceptance of the right to autonomy and self-determination;[19] crucial factors to childhood development. As individual rights-holders, children should be able to exercise these Rights and Freedoms to their fullest extent while maintaining the "greatest possible access to Internet-based content, applications, and services."[20] Even an account deactivation could constitute as an interference with these Rights and Freedoms.[21]

Both the EDPS and EDPB have also made clear that organisations should not legitimately be allowed to deny access to a service when an individual does not give his or her consent for data processing outside of what is necessary to deliver the service to the user.[22] In light of the foregoing, it is our view that any policy that locks users out of a service purely on the basis that a user does not give consent for data collection would inappropriately override other Fundamental Rights.

---

[9] Council of Europe, Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to Human Rights for Internet Users, 2014, para 32

[10] United Nations Convention on the Rights of the Child (UNCRC) 1989, Art 13(1); Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as Amended) (ECHR) 1950, Art. 10(1), European Union, Charter of Fundamental Rights of the European Union (Charter) 2000, Art. 11

[11] UNCRC, Art. 15(1); ECHR, Art. 11(1); Charter, Art. 12

[12] UNCRC, Art. 16(1); ECHR, Art. 8(1); Charter, Art. 7

[13] Charter, Art. 8

[14] UNCRC, Art. 17

[15] UNCRC, Art. 13(2); ECHR, Art. 10(2)

[16] UNCRC, Art. 15(2); ECHR, Art. 11(2)

[17] ECHR, Art. 8(2)

[18] Niemetz v Germany, no. 13710/88, para 29; X v Iceland, no. 6825/71, Commission Decision 18 May 1976

[19] BVerfGE 65, 1 – Volkszahlung Urteil des Ersten Senats vom 15. Dezember 1983 auf die mundliche Verhandlung vom 18. und 19. Oktober 1983

[20] Council of Europe, Compass: Manual for Human Rights Education with Young People, available at <https://www.coe.int/en/web/compass/media> accessed February 20 2019

[21] See n. 15, para 53

[22] European Data Protection Supervisor, Opinion 6/2017, EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation); Article 29 Working Party, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), para 20

Our practical recommendation is that any service providers who are aware of a user who is under 16, should be required to adapt their service to either:

A. Limit data collection and processing activities to those for which they have a legal basis other than consent (e.g. Legitimate Interest); and/or

B. Implement a verifiable parental consent mechanism to enable any data collection or processing that cannot be done on another legal basis

Our experience in working with both child-directed as well as mixed-audience apps and websites indicates that most have the ability to restrict features of their service, with reduced data collection when required to do so. We would therefore recommend that service providers instead adapt their services accordingly.

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

The compliance burden associated with applying different age thresholds in each country is significant as it would require further expense, is technically complex, and creates a substantially higher risk of error. We therefore recommend a pragmatic and safety-first approach which takes this into account. As such, we have been advising many service providers in the past year on the best way to approach the different ages of consent across the EU. Our evolved view and recommendation to publishers (websites and apps) is to ignore the varying age thresholds and instead apply the highest common denominator (age 16) across the territory.

5. **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?**

Recital 47 of the GDPR notes that the processing of personal data for marketing purposes may be regarded as a legitimate interest. It is our opinion that, when taking Recital 38 into account, there should be very few scenarios where this should be applicable in relation to children.

Online advertising is today primarily delivered via the use of behavioural targeting (whereby users are delivered ads based on personal profiles derived from online shopping and online browsing behaviour). However, the DPC must understand that in order to deliver online advertising, advertisers need to process personal data for various other reasons to ensure that ads:

- Are delivered to a human and not a "bot" ('inhuman traffic detection' or 'IVT')
- Have the opportunity to be seen by a human ('viewability')
- Are not delivered more often than necessary to an individual ('frequency capping')
- Are displayed against suitable content ('brand safety')

These purposes require the use of online identifiers or device information but not in connection with the profiling of individuals or the selling of personal data. These processing activities serve internal operational purposes (of the advertiser) and do not have a legal or other similarly significant effect on the user. In taking Recital 38 into account, we *would* consider that these purposes indeed, fulfill a legitimate interest. These scenarios are similar to the Federal Trade Commission's specific exemptions for "internal purposes" under COPPA[23] which has served to be an effective and pragmatic approach. We urge the DPC to consider a similar clarification regarding when legitimate interest is acceptable in relation to marketing to children.

We firmly believe that, subject to service providers completing an appropriate balancing test, the provided framework (*see Table 2*) will assist in illustrating the aforementioned point.

Table 2 Purposes and examples where a Legitimate Interest may apply

Data type	Purpose	Examples	Risk	Legal basis
IP address or device ID or other technical identifier	Personalisation	Site remembers games scores, or user choice of background colour	Low	Legitimate Interest
IP address or device ID or other technical identifier	Analytics, security, internal operations	Pseudonymised (and often aggregated) data used by ISS to improve service, enable auto-scaling, provide business analytics internally	Low	Legitimate Interest
IP address or device ID or other technical identifier	To serve advertising based on context of the site; to frequency-cap such advertising messages within the domain	An app or websites that funds itself primarily through advertising	Low	Legitimate Interest
Geolocation (based	At country- or	Film studio website	Low	Legitimate Interest

[23] Federal Trade Commission, Complying with COPPA: Frequently Asked Questions A Guide for Business and Parents and Small Entity Compliance Guide (2015), available at <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions> accessed February 19 2019

on IP address or GPS)	city-level only, for purposes of tailoring content to the user, eg personalisation	that shows a trailer for a film in theatres in one country, which may not yet be available in another.		
Device information including user agent (technical configuration)	To detect language settings and browser type, for user experience	Game that can be delivered in the language of the user, and is optimised to work with the user's specific browser	Low	Legitimate Interest

6. 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?

Article 22 of the GDPR does not explicitly prohibit solely automated decision-making (including profiling) where children are involved if it does not have a legal or similarly significant effect. We acknowledge that Article 22(2)(b) allows Member States to lay down by law, suitable measures to safeguard an individuals' rights and freedoms in this regard. However, as aligned with the CoE[24] and EDPB,[25] we do not feel that organizations should be granted the ability to profile children for direct marketing purposes.

It has been found that in many instances, children do not intuitively regard their social online interactions as being subjected to ongoing monitoring[26] despite research to indicate their increasing awareness of such commercial practices.[27] Though we recognize that children of varying ages possess different cognitive development stages and understanding,[28] there should be no justification to allow the profiling of children of any age since such commercial practices tend to have negative effects,[29] primarily due to a lack of experience and maturity. We are further concerned that by allowing such practices, organizations may feel tempted to collect additional data or make further inferences in an attempt to create new revenue streams given the spending power that children possess.[30]

---

[24] Council of Europe, Recommendation CM/Rec(2018)7 of the Committee of Ministers Guidelines to Respect, Protect, and Fulfill the Rights of the Child in the Digital Environment (2018), p. 17

[25] Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (2018), p. 29

[26] Grace Chung and Sara M. Grimes, Data Mining The Kids: Surveillance And Market Research Strategies In Children's Online Games (2006) 30 Canadian Journal of Communication

[27] Sonia Livingstone, Mariya Stoilova, Ritisha Nandagin, Conceptualising Privacy Online: What Do, and What Should, Children Understand? (LSE, 2018) available at <https://blogs.lse.ac.uk/mediapolicyproject/2018/09/07/conceptualising-privacy-online-what-do-and-what-should-children-understand/> accessed February 22 2019

[28] *Ibid.*

[29] *Ibid.*

[30] Simone Van der Hof, 'Agree, Or Do I: A Rights-Based Analysis Of The Law On Children's Consent In The Digital World' (2017) 34 Wisconsin International Law Journal; Jerry Daykin, Personalised marketing at scale is the next big thing in digital (The Guardian,

7. 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?

Most simply, organizations that offer services or products to children should take Privacy by Design (PbD) concepts seriously. PbD is a *proactive* measure which stipulates that 'privacy' should be embedded at the design phase of ICT systems, should facilitate end-to-end security, and should be "on" as default to fully respect user privacy.[31]

At its core, this would mean that PbD principles are hardcoded into all software or applications which make up a product or service. This is easier said than done as it is often difficult to bridge the abstract notion of 'privacy' into concrete technical rules. Furthermore, limitations in products such as IoT devices or connected toys due to processing power constraints, reliance on third-party infrastructure (which likely does not incorporate privacy-enhanced architectures), and a rush to market usually mean that PbD remains an "afterthought".

In the online world, digital profiles are built upon identifiers that, while not directly identifying an individual,[32] are *attributable* to an individual. The risk to privacy[33] is derived from storage and data processing practices when multiple, seemingly "anonymous identifiers"[34] are collected ubiquitously (as is common) over a period of time, combined with other seemingly anonymous data from other sources, and assembled into digital profiles.

The threat to privacy is further magnified by the growing frequency of data breaches.[35] For context, the EDPB has reported a significant increase in breach reports, around 41,502 from 25 May 2018 to the end of January 2019[36] across Europe while the ICO has reported it has received more than 8,000 reports by the end of 2018.[37]

2015), available at <https://www.theguardian.com/media-network/2015/mar/19/personalised-marketing-digital-future> accessed February 21 2019

[31] Ann Cavourkian, Privacy by Design The 7 Foundational Principles, available at <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf> accessed February 22 2019

[32] For example, an actual namel; although we do note that depending on the product or service, this type of data may be collected and stored against device identifiers such as an IMEI number upon product registration

[33] Such as re-identification or accidental sensitive inferences

[34] We recognize that these pieces of data are in fact, pseudonymous in nature

[35] As opposed to a data leak

[36] European Data Protection Board, GDPR in Numbers, available at <https://ec.europa.eu/commission/sites/beta-political/files/190125_gdpr_infographics_v4.pdf?utm_medium=social&utm_source=linkedin&utm_campaign=postfity&utm_content=postfity05e1e> accessed February 21 2019

[37] ICO,International Privacy Forum (December 2018), available at,<https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/12/international-privacy-forum-forum/> accessed February 22 2019

Effective PbD does not necessarily mean the use of only technical solutions but must incorporate organizational measures as well. Organizations should therefore implement the following controls, especially where products or services are offered to children:

- **Minimize**: reduce the amount of data collected at first instance and/or minimize the use of the data
  - Exclude or select to collect only certain types of data (at the point of collection)
  - Strip unnecessary fields for the processing purposes
  - Opt to process data on the user's device, rather than transfer such data to an additional system

- **Control access**: prevent exposure of data
  - Restrict access to the data itself
  - Mix (by injecting additional or other data points into the datasets) or obfuscate (encrypt or hash) data using various de-identification techniques (ideally end-to-end encryption)
  - Dissociate data by removing any correlation between various pieces of data

- **Separate**: prevent data correlation by distributing or isolating the storage of personal data
  - Distribute data by partitioning it across separate data stores with various access restrictions (ideally separate data stores for unique identifiers and data events)
  - Isolate data by processing only specific parts of the personal data

- **Aggregate**: limit the amount of detail of the data
  - Summarize data so that only correlations in the data are processed
  - Group data by allocating personal data based on common categories

- **Enforce**: contracts and legal obligations
  - Create, maintain, and uphold policies and technical controls with regards to collection, storage, retention, sharing, operations, etc.

Underlying the above recommendations is for organisations to take an architectural approach that separates personal data, including pseudonymous identifiers, from event data. Instead, systems should be designed in such a way that data can be used within the scope for which it was initially collected, but isolated in such a way to make it difficult for misuse by third parties, even in the event of a data breach.

8. **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?**

It has been well documented that children of varying ages possess different levels of maturity, capacity, and understanding.[38] It is therefore correct to state that a five-year old does not possess the same level of understanding or have the same needs as a ten-or fifteen-year old and should not be treated the same.

Practically, it is not sensible to separate children into specific age groups for the purpose of providing variations in privacy settings. Service providers would have to adapt their approach at a granular level to accommodate different age groups which would result in the collection of additional personal data. We would further caution the DPC with this approach as it could also mean falling into an outdated "ages and stages" developmental psychology theory.

The data privacy protections that have been discussed at length in this consultation are ones that we believe **should apply to all children under the age of consent.** This includes a prohibition on profiling and a restriction on the processing of data without verified parental consent. Service providers should be applying the highest standard of data privacy protections when offering services to children by ensuring that privacy notices are transparent and understood by their primary audiences (including children) and, where appropriate, the parents of pre-reading age children.

[38] Sonia Livingstone, Mariya Stiolova, Ritisha Nandagiri, 11 Key Readings on Childrens Data and Privacy Online (LSE, 2018) available at,<https://blogs.lse.ac.uk/mediapolicyproject/2018/12/18/11-key-readings-on-childrens-data-and-privacy-online/> accessed February 20 2019