GDPR Implementation
In Respect of Children's Data and Consent

Centre for Information Policy Leadership

6 March 2018

CIPL's TOP TEN MESSAGES ON GDPR IMPLEMENTATION IN RESPECT OF CHILDREN'S DATA

1. **While Article 8 of the GDPR imposes specific conditions to a child's consent in relation to the offer of information society services directly to a child, other legal processing bases are still applicable and sometimes more appropriate to the processing of children's data.**

2. **The offer of an information society service directly to a child neither means "offered exclusively" to a child nor does it mean "made available" to a child. Rather, it is a contextual determination that must be made through an appropriate risk-based test.**

3. **A risk-based test to determine whether an information society service is offered directly to a child should be developed within the framework of the GDPR, taking into account whether the offering is made intentionally attractive to children.**

4. **A widely recognised, effective and reliable method of parental verification which can be applied globally should be supported by regulators and developed together with industry.**

5. **Where the holder of parental responsibility gives or authorises consent for processing a child's personal data under Article 8, such consent should remain valid when the child attains the age of digital consent.**

6. **Organisations should have the flexibility to provide transparency and notices in the way they think is most appropriate to cater to their specific audience, taking into account that the audience may include young children.**

7. **In general, the processing of 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.**

8. **The importance of a consistent approach to implementing national age thresholds should be emphasised by data protection authorities in line with the GDPR's goal of harmonisation. This is particularly relevant as Member States finalise their national data protection laws implementing the GDPR.**

9. **The age at which children can exercise their rights under the GDPR (apart from consent under Article 8) turns on questions of competence which are issues of Member State law.**

10. **Providers of information society services, which fall within the scope of Article 8, should be permitted to rely on legitimate interest for the continuation of services to children, who previously consented to processing by the service, after 25 May 2018, provided the requirements surrounding the use of the alternative legal basis are met.**

I. Introduction

Personal data relating to children are processed for many purposes by private and public sector organisations, including the provision of online and offline services, education, social care, healthcare and personal welfare, and as part of information on family circumstances. In some cases, the processing will include special categories of personal data. CIPL recognises that the processing of children's personal data may be regarded as high risk in some cases and require particular levels of care. Indeed, the importance of protecting the rights of children has been highlighted by Article 24 of the EU Charter of Fundamental Rights.[1]

Numerous working documents and initiatives regarding personal data relating to children under the GDPR have been released by data privacy regulators for public consultation. Notably, on 28 November 2017, the Article 29 Data Protection Working Party (WP29) issued for consultation its guidelines on consent[2] detailing specific issues relating to children within the broader context of consent. Similarly, use of children's personal data for profiling is also addressed in the WP29 guidelines on automated individual decision-making and profiling.[3] In addition, on 21 December 2017, the UK Information Commissioner (ICO) issued a consultation document solely focused on the GDPR's application to children's data[4] (ICO Consultation).

Furthermore, in preparation for the GDPR, significant legislative developments specific to children are beginning to take shape at national level. For instance, many Member States, in creating, updating and/or amending national data protection laws have made use of the margin of manoeuvre afforded to them under Article 8(1) of the GDPR. Selection of the age of digital consent, within the 13-16 threshold range, varies widely among the Member States.[5]

---

[1] 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.

[2] WP259 Guidelines on Consent under Regulation 2016/679 at p. 23-27, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849.

[3] WP251 Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826.

[4] Information Commissioner's Office, Consultation: Children and the GDPR guidance, https://ico.org.uk/media/about-the-ico/consultations/2172913/children-and-the-gdpr-consultation-guidance-20171221.pdf.

[5] At the time of writing, only Austria and Germany have finalised their national privacy legislation in line with the GDPR and chose the following age thresholds – Austria (14) and Germany (16). Several other Member States have released draft bills which are currently going through national legislative procedures. The age thresholds for these Member States include: Czech Republic (13); Denmark (13); Ireland (13); Latvia (13); Poland (13); Spain (13); Sweden (13); UK (13); Hungary (16); Lithuania (16); Luxembourg (16); Slovakia (16); and the Netherlands (16).

In this paper CIPL addresses issues raised by the processing of personal data relating to children[6] by private sector organisations, such as service providers in the online environment, typically for activities such as social media, the use of some online games or certain IoT products, online advertising services or e-commerce sites which can be used by children, for example by the use of pre-paid debit or gift cards.

With the GDPR adopting a squarely risk-based approach, CIPL considers it important to recognise that not all processing of personal data relating to children raises the same levels of risk. Article 5 of the GDPR includes the overarching principles relating to the processing of personal data. Among them are the principles of fairness, transparency and accountability. In determining what is required to achieve compliance with these overarching principles, regard should be had to the particular risk in order to determine a proportionate approach and specific compliance steps. CIPL's view is that there should not be an assumption that there must be one standard approach to dealing with children's data.

II. Relevant Provisions in the GDPR

Recital 38 recognises that "children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data". Recital 75, which explains criteria for the risk-based approach, specifically mentions children as vulnerable natural persons.

Most of the provisions, however, do not distinguish between different ages[7] and are equally applicable to all across the board. Additionally, questions of legal competence based on age are generally matters for Member State law. Nevertheless, the GDPR does set out several important provisions related to children and these provisions raise a multitude of issues which are further explored in this paper:

- **Article 8** sets out a provision on conditions applicable to a child's consent to the processing of their personal data in relation to information society services (ISS(s)) offered directly to a child.

- **Article 6(1)(f)** with regard to the legitimate interest balancing test specifically notes that processing can take place for the legitimate interests pursued by the controller "except

[6] This paper responds to issues about the processing of personal data relating to children under the GDPR generally and also addresses several issues raised by the WP29 in their Guidelines on consent (see footnote 2) and the UK ICO Consultation on children and the GDPR (see footnote 4).

[7] The Commission proposal for the GDPR specifically defined a child as "any person below the age of 18 years". However, this was removed from the final text. This definition was based on the United Nations Convention on the Rights of the Child (UNCRC). See https://downloads.unicef.org.uk/wp-content/uploads/2010/05/UNCRC_united_nations_convention_on_the_rights_of_the_child.pdf?_ga=2.137520179.2061360723.1518114958-1215330260.1518114958.

where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child" (Emphasis added).

- **Article 12** on providing transparent information specifies that "the controller shall take appropriate measures to provide [the individual with information required by the GDPR] in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child" (Emphasis added).

  Recital 58 notes that, given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

- **Article 17(1)(f)** explicitly references children in respect of the right of erasure. Article 17(1) provides that an individual shall have the right to erasure of personal data concerning him or her where one of the Article 17(1) grounds applies. Article 17(1)(f) specifies that the right to erasure exists where the personal data have been collected in relation to the offer of ISSs referred to in Article 8(1) (i.e. where the processing is based on consent and such consent has been given or authorised by the holder of parental responsibility (HPR) for a child under the age of digital consent in Member State law).

  Recital 65 states that erasure is particularly relevant where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The Recital further notes that the data subject should be able to exercise the right of erasure notwithstanding the fact that he or she is no longer a child.

- **Article 22** on automated decision-making, while it does not reference children directly, is of relevance as Recital 71 states that "such measure should not concern a child". Nevertheless, the WP29 guidelines on automated decision-making specify that this is not to be interpreted as a blanket prohibition for automated decision-making with regard to children's data.[8]

- **Article 40(2)(g)**, on codes of conduct, states that associations and other bodies representing categories of controllers or processors may prepare codes of conduct or amend or extend such codes, for specifying the application of the GDPR with regard to the information provided to, and the protection of children, and the manner in which the consent of the HPR is to be obtained.

[8] See footnote 3 at page 28.

- **Article 57(1)(b)** states that each supervisory authority shall on its territory promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention.

III. Legal Basis for Processing

Article 8 of the GDPR imposes specific conditions applicable to a child's consent where a controller relies upon consent (Article 6(1)(a)) as a basis for processing in relation to the offer of an ISS directly to a child. However, it is important to recognise that the other legal bases of processing are still applicable and in some cases may be more appropriate to the processing of children's data.

For instance, the ICO notes that consent may be inappropriate if there is an imbalance of power between the child and the ISS but gives no examples of this. The issue of consent and the imbalance of power is usually referred to within the employment context (which is generally not applicable to children) and for processing by public authority controllers. It would be helpful to have some examples of the ICO's thinking on this point as it relates to children. Clearly, in such circumstances an alternative processing ground, if applicable, would be more appropriate.

CIPL acknowledges and agrees with the ICO Consultation which points out that contractual necessity as a legal ground for processing (Article 6(1)(b)) can be applied where the child is competent to enter into contracts under Member State law and that this point should be considered by the controller. Equally, the ICO recognises that it is possible to rely on the legitimate interest processing ground (Article 6(1)(f)) but notes that the balancing test must be carefully applied and any risks must be mitigated, as far as possible. For example, when a child engages with an ISS by downloading and using an app, there are identifiers associated with that download and usage. Processing such identifiers to improve the functionality of the app for the user is likely a legitimate interest of the controller which must undergo the appropriate balancing test. In many cases, a controller's use of legitimate interest requires deeper thinking and strategizing and more care to correctly implement than seeking consent alone and should be encouraged as a lawful basis to process children's data in appropriate circumstances.[9]

In summary, the GDPR does not limit the processing of childrens' personal data to the consent processing ground alone and other legal bases, such as legitimate interest, can be used for such processing in appropriate circumstances. CIPL recommends that regulator guidance

[9] Given that the legitimate interest ground requires a risk assessment and a balancing of interests, coupled with appropriate mitigations and accountability from controllers, it provides a robust framework for considering risk on a case-by-case basis and allows for specific risks to be addressed in specific contexts (i.e. such as those relating to the interests or fundamental rights and freedoms of children).

acknowledge this fact and stress that it is the controller who must determine the most appropriate legal basis or bases for their specific processing operations, within the context of the GDPR. Such guidance should also provide examples of different contexts where other processing grounds apply in relation to processing children's data. Finally, the ICO should clarify what contexts constitute an imbalance of power between a child and an ISS which would result in consent being an inappropriate ground for processing.

IV. Article 8

Article 8 of the GDPR introduces a higher threshold of protection for the processing of children's data where the processing is related to the offer of an ISS directly to a child and the processing is based on consent. Where the child is below the age of 16 (or lower, in accordance with Member State law, but not lower than 13) the processing is only lawful "if and to the extent that consent is given or authorised by the HPR over the child."

While Article 8 does not make reference to the processing of special categories of personal data of a child under Article 9, nothing suggests that Article 8 applies to non-sensitive data only. As the requirements of Article 6(1)(a) and Article 9 are cumulative, CIPL believes the rules of Article 8 apply equally to both sensitive and non-sensitive children's data. As with all cases of sensitive data processing, obtaining valid consent requires the consent to be "explicit".[10] However, it is important to note that this higher bar for consent is only required in the context of Article 8 when sensitive data are processed.

Article 8(2) requires the controller to make reasonable efforts to verify that consent is given or authorised by the HPR over the child, taking into consideration available technology.

Article 8 only applies where the ISS provider processes personal data of the person using the service. In addition, Article 11 states that "if the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation". It is possible that an ISS provider may be able to offer the service without collecting or processing data which is identifying or makes the user identifiable, e.g. a free online game that does not require user registration or the input or collection of any personal data to use the service.

[10] For a full discussion of obtaining explicit consent, please see CIPL's comments to the WP29 Guidelines on Consent at page 14, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_wp29_guidelines_on_consent-c.pdf.

V. The Offer of Information Society Services Directly to a Child

a. Meaning of "Information Society Service"

The obligations under Article 8 apply only where information society services are offered directly to a child. "Information society services" are defined by reference to Directive 2015/1535 1(1)(b).[11] The definition specifies than an ISS is any service provided at a distance, by electronic means, and at the individual request of a recipient of the services. This would seem to cover most digitally delivered services including screenless devices. The definition also includes the requirement that the service be one normally provided for "remuneration". In general, the approach to this requirement has been to take a broad view of the term, in line with the broad notion of services in EU law, so that any service which supports a business is regarded as covered.

There is an open question as to whether a non-profit organisation providing a service at a distance, by electronic means and at the individual request of a recipient of the services, would be considered an ISS. These services are, by their nature, not normally offered for remuneration. While it is true a service does not necessarily require an individual to make a payment for the service to be considered an ISS, regulators should clarify in what circumstances they consider non-profits are likely to fall within the scope of the definition of an ISS.

Additionally, Recital 38 of the GDPR notes that the consent of the HPR should not be necessary for preventative or counselling services offered directly to a child. Such services may be considered an ISS if they meet the relevant criteria laid out in Directive 2015/1535 1(1)(b) but nevertheless fall outside the scope of Article 8.

b. Online and Offline Services

In a recent case[12] before the European Court of Justice (ECJ), the question of whether services with both online and offline components are considered to be ISSs was discussed. The ECJ ultimately held that a service for peer-to-peer ridesharing which functions through a location-based app was not an ISS, despite it having an online app component, as the main component (i.e. the transportation service) is not an ISS. The ruling provides some insight for service

[11] Directive 2015/1535 1(1)(b): 'service' means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of this definition: (i) 'at a distance' means that the service is provided without the parties being simultaneously present; (ii) 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; (iii) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request. See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_241_R_0001.

[12] Case C-434/15, Asociacion Profesional Elite Taxi v Uber Systems Spain SL, ECLI:EU:C:2017:981.

providers and an examination of whether their online service components form an integral part of their overall service will be critical to determining whether the service is considered to be an ISS. This question is relevant for many e-commerce sites and further raises the question of whether a connected device (i.e. a device that communicates via Wi-Fi to an app across the internet) which collects personal data is considered an ISS.

In summary, it is not clear whether certain services constitute an ISS. In particular, guidance on whether services provided by non-profits, services with online or offline components and connected devices constitute ISSs would be helpful.

c. Offering an ISS Directly to a Child

Once it is determined whether the service in question constitutes an ISS, the question, for purposes of Article 8 GDPR, is whether the ISS is offered directly to a child.

While the GPDR specifically refers to the definition of an ISS in Directive 2015/1535, the terms "offer" and "directly" are not defined by the GDPR, nor is any reference made to other legislation which defines these terms. It appears that the question of whether an ISS is offered directly to a child will be primarily a question of fact. ISSs expressly designed for those over 18, such as gambling and other sites which are "hard age-gated",[13] fall outside the scope of Article 8 as these are not offered directly to a child. On the other hand, ISSs which are intentionally designed for children clearly fall within the scope of being offered directly to a child.

The key issue arises around ISSs that are designed for a universal audience, which includes children as a subset. "Offered directly to" does not mean "made available to" or "offered indirectly to" as that could include all services which a child can access even if the ISS is not intended for a child's use. The choice of including the words "offered directly" in Article 8 reflects a pragmatic choice by the drafters to limit the application of Article 8 to services that are specifically intended to be offered to children. This choice should be honoured by the WP29[14] in its interpretation of the meaning of "offered directly to a child".

Current guidance by the WP29 does not address the issue of such mixed audience services but rather addresses the clear-cut case of ISSs directed to adults which are hard age-gated.

The WP29 guidelines state:

> In this respect if an information society service provider makes it clear to potential users that it is only offering its service to persons aged 18 or over, and this is not undermined by other evidence (such as the content of the site or marketing plans) then the service will not be considered to be 'offered directly to a child' and Article 8 will not apply.

[13] E.g. By requiring the production of a credit card in the name of the user.
[14] Where this paper addresses the WP29, it should be noted that we are also addressing the future EDPB.

Reference is made only to services which are hard age-gated to those over 18. The guidelines do not, however, address the specific problem of an ISS that offers a general service which neither explicitly targets children (for example by means of its content) nor clearly excludes them.

Guidance by the ICO also addresses services which are made available to users who are age 18 and over but additionally states that any ISS made available to all users is considered as being offered directly to a child.

The ICO guidance states:

> The Commissioner also considers an ISS (online service) is offered directly to a child when it is made available to all users without any age restrictions or when any age restrictions in place allow users under the age of 18.
>
> If an ISS (online service) is only made available to users who are aged 18 and over then it is not being offered directly to a child. However, if your ISS (online service) states that it has such an age limit then, in the event of a complaint, the Commissioner may look for evidence that the limit is applied in practice, and not just in theory, when deciding whether Article 8 applies. She may consider evidence such as site content, marketing plans, systems or processes designed to limit access, and information provided to users, in this respect.

While it is true that "offering directly" does not equate to "offering exclusively", CIPL disagrees with the proposition that simply making an ISS available to those under 18 means that the ISS is offered directly to a child. Such a proposition expands the scope of Article 8 to potentially every ISS without stringent age verification mechanisms in place, even where the service is agnostic towards the age of its users (for example, in cases of OTT messaging or email services). A comparison can be made to the offer of goods and services generally to individuals in the Union. Recital 23 notes that the mere accessibility of the controller's website (where the controller is established outside the Union) by individuals in the Union is insufficient to ascertain an intention to offer goods and services to individuals within the Union.[15] However, factors such as the use of local languages or currency used in one or more Member States may make it apparent that the controller envisages the offering of goods or services to individuals in the Union. Equally, the mere accessibility of a controller's online service by children does not make it apparent that the controller envisages offering the service directly to children. CIPL proposes a pragmatic approach, which takes into account relevant factors, to make such a determination (see Section VI below).

[15] See also Case C-101/01, Lindqvist, ECLI:EU:C:2003:596.

With respect to the ICO's statement that the Commissioner may look for evidence that age limits are applied in practice regarding ISSs offered to those over 18, CIPL believes that this is a reasonable approach but the burden of restricting access should be proportionate to the nature of the site and the service or material which it provides. In certain cases, a clear statement in the terms of service combined with a policy to exclude any user under the age of 18 should be sufficient.

VI. ISS Directed to All Users – Developing Tests on the Application of Article 8

In relation to consent-based services which do not fall into either of the clear categories of being specific to children below the threshold age (i.e. where there is no doubt that consent must be given or authorised by the HPR) or are hard age-gated (i.e. where the service clearly falls outside the scope of Article 8), there has been little discussion on the factors which are relevant for determining whether an ISS is offered directly to a child.

a. Approach 1: Universal Age Assessment

The first approach to consider is that an ISS which is not hard age-gated (i.e. not restricted in a way that allows only adults to access it) is one that is being offered to all individuals and this includes children. Such an ISS would fall within the scope of Article 8 and age assessment would be required in all cases.

The problem with this approach is that it means all ISSs which are not hard age-gated potentially require some degree of age assessment. This would include all public service sites, academic sites and business sites that rely on consent for the processing of data and that fall within the definition of an ISS. It would require all ISSs to collect some personal data about all visitors, even if only a statement by a visitor that he or she is over 16 (or the relevant age in the Member State). This raises serious questions over data collection which goes against the principle of data minimisation and becomes almost a surveillance issue.

The WP29 guidelines on consent support this approach and note that "although the need to verify age is not explicit in the GDPR it is implicitly required...". However, Article 8, by its terms, does not require general age verification of all users of ISSs. Rather, Article 8 requires that consent be given or authorised by the HPR of a child below the threshold age where an ISS provider offers its service directly to a child and processes the child's data based on consent. The requirement that a provider of an ISS ensures it only engages an age-verified user, is not contained within the GDPR.

The GDPR does include an explicit obligation to make reasonable efforts to "verify" that consent is given or authorised by the HPR but does not include the same obligation regarding the age of a user of an ISS. If such a verification obligation was intended it would impose a significant duty and as a matter of drafting it would be expected that such a requirement would

be explicit in the wording used in Article 8. The statement by the WP29 that this obligation is "implicit" in all cases expands the obligations of Article 8 beyond those imposed by the GDPR. The fact that the consent-based processing of personal data of a child might be unlawful without valid parental consent is not sufficient to create a positive obligation to verify age in all cases.

In summary, this approach is over-inclusive.

b. Approach 2: Limited Age Assessment

An opposing view is that only those services which state overtly that they specifically intend to target children under the relevant age threshold should be regarded as offering ISSs directly to a child.

While it is true that "offered directly to a child" is a higher bar than merely making an ISS available to them, the problem with this approach is that many ISSs which do not state overtly that they are targeted at and intended for children may nevertheless be designed to be intentionally attractive to children and incorporate various factors which demonstrates this. For example, children's cartoon characters or child celebrities. This runs the risk that a provider of an ISS which is in fact offered directly to a child can evade the obligations of Article 8 by simply ensuring the service doesn't overtly state it intends to target children.

In summary, this approach is under-inclusive.

c. Alternative approach

CIPL believes a more suitable, realistic and helpful approach to the application of Article 8 is the incorporation of a risk analysis, based on evidence, in determining whether an ISS is offered directly to a child. Such an approach avoids a general requirement to verify the ages of all users. CIPL recommends this approach be further explored by regulators and impacted organisations.

CIPL has considered how this approach might be developed within the framework of the GDPR. One possibility would be to interpret the phrase "offer of ISSs directly to a child" as creating a specific test where: (i) the nature of the ISS offered; (ii) the accessibility of the service (bearing in mind that services must also comply with accessibility obligations); and (iii) the potential attractiveness of the service to children should be considered. Such a test, conducted periodically, as appropriate, could take into account factors such as:

- Whether the offering is intentionally made to be attractive to children;
- Whether children have been attracted to the ISS or similar services in the past; and

- Whether the registration process to the ISS reflects an assumption that the users are above the age of digital consent.

In determining the parameters of the test, the United States' approach under the Children's Online Privacy Protection Act (COPPA) provides a useful reference. Under US law, a website or online service "directed to children" must obtain parental consent prior to collecting personal data from children under 13. In that case, "directed to children" does not mean merely "making available" to children but rather, "targeted to children," based on a set of enumerated criteria. The criteria include: The subject matter of the site or service, the visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, the age of the models, presence of child celebrities or celebrities who appeal to children, the language or other characteristics of the website or online service, whether advertising that appears on the site or service is directed to children and empirical evidence regarding audience composition or the intended audience of a site or service.[16] US ISSs use these criteria in designing their services, and the US Federal Trade Commission (FTC) applies these criteria in bringing its enforcement actions.

Similar criteria are used in the UK to determine whether an online game or app is likely to appeal to children.[17] The criteria include the inclusion of characters popular with or likely to appeal to children, cartoon-like graphics, bright colours, simplistic gameplay and/or language; if the game concerns an activity that is likely to appeal to or be popular with children; if the game is available to be downloaded, signed up to or purchased by anyone and is not age-restricted; and if the game is featured in a children's section of an app store. Importantly, the fact that the online game or app is not age restricted and is available to anyone is just one factor in the determination and not decisive in its own right.

A similar set of factors could be looked at by ISSs seeking to determine whether their service falls within the scope of Article 8 (i.e. is offered directly to a child). Developing guidance on such factors and a set of highly detailed FAQs[18] should be a top priority for the EDPB and these should be carefully formulated in conjunction with input from industry.

The test should also take into account that an ISS may be part of a larger offering or site. As an example, a fast food restaurant might have a large website offering goods and services catered to all users with one section devoted to online games for children. It should be clear that only

[16] See 16 US Code of Federal Regulations § 312.2 (Definition of "website or online service directed to children"), https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5#se16.1.312_12.

[17] See the Office of Fair Trading Principles for Online and App-Based Games, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/288360/oft1519.pdf.

[18] Inspiration can be drawn from the approach of the US Federal Trade Commission. See "Complying with COPPA: Frequently Asked Questions", https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

the specific ISS offered directly to children would be covered by Article 8, in this case the online gaming portion of the site (in so far as the related data processing relies on consent). However, organisations should still conduct a risk assessment, in line with the test put forward in this section, in respect of their whole ISS to make that distinction. In the example, the risk assessment should cover the entire fast food website.

The test could also be accompanied by further safeguards. For example, a requirement on ISS providers to retain current and/or periodically updated evidence of their assessment of the nature of the ISS in relation to Article 8 so it can be checked by the competent supervisory authority.

This approach would remove from consideration services which are not in any way aimed at children or are unlikely to be attractive or accessible to them or in any way interesting but are not hard age-gated to prevent children actually accessing them (e.g. law firm, public services or university-level academic sites and many business sites which fall within the definition of an ISS).

Both the WP29 and the ICO endorse incorporating elements of risk assessment into the determination of whether Article 8 is applicable to an ISS. However, the current guidance does not fully distinguish the assessment of whether an ISS falls within the requirements of Article 8 from the subsequent question of whether, and if so how, collection of age information is required. CIPL believes it is crucial that a clear separation is made between questions regarding the scope of Article 8 and questions of collecting age information, particularly because the latter is not required by the GDPR.

The ICO incorporates a risk analysis, by advising that if a data controller is not sure whether users of the service are children, a cautious approach should be adopted. It suggests options such as:

- Designing processes to provide sufficient protection;
- Putting in place proportionate measures to prevent or deter children;
- Taking action to enforce age restrictions; and
- Implementing up front age verification systems.

The ICO suggests that the relevant options may vary, dependent on the risks of the processing and how attractive the site is.

The WP29 states:

> Age verification should not lead to excessive data processing. The mechanism chosen to verify the age of a data subject should involve an assessment of the risk of the proposed processing. In some low-risk situations, it may be appropriate to require a new subscriber to a service to disclose their year of birth or to fill out a form stating they are (not) a minor. If doubts arise the controller should review their age verification mechanisms in a given case and consider whether alternative checks are required.

CIPL appreciates the WP29's and ICO's recognition of the importance of a risk assessment for purposes of Article 8. However, 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.

VII. Parental Verification

Where an appropriate risk assessment has been carried out and indicates that an ISS is offered directly to a child, then consent to the processing shall only be lawful if it is given or authorised by the HPR.

In its consent guidelines, on page 26, the WP29 suggests that the method for verifying that consent is given or authorised by the HPR should depend on the underlying processing at issue, in particular whether the processing may be regarded as low-risk or high-risk processing. The ICO Consultation also considers the practical problems of verification and the concept of reasonable effort. The ICO considers that the level of reasonable effort required should take account not only of the available technology but also of the level of risk involved in the processing.

There is some ambiguity in Article 8 as to whether this is a risk-based test. The obligation in Article 8(1) is that the HPR must give or authorise consent for the processing. This is not dependent on the underlying data processing at issue. Article 8(2), however, requires the controller to make "reasonable efforts" to verify that the consent is given or authorised by the HPR, taking into account available technology. It does not refer to the concept of the risk of the processing. Both the WP29 and ICO appear to have taken the view that regard has to be had to whether the controller's efforts are reasonable in all the circumstances and whether the nature of the processing involved would be relevant to this test. Therefore in those cases where the processing is low risk, for example there is minimal collection of personal data from the child for an obvious and specified purpose, it is possible that a controller may consider a lower level of verification.

CIPL supports the view that the method for verifying parental consent can be risk related, as further explained below.

VIII. Methods of Verification

The options for methods of parental verification are potentially wide. There is discussion over when parental verification can be based on simply an email exchange or requires additional proof. The WP29 provides examples which could include, relying on existing credit card or other payment instrument information from the parent instead of requiring a bank transaction. Some providers will have implemented verification methods to comply with COPPA in the US. The US FTC has made clear that the basic standard is "reasonable assurance" that the person the ISS is dealing with is the parent of the child.[19] Similarly, Article 8(2) of the GDPR requires controllers

[19] See 16 U.S. Code of Federal Regulations § 312.5(b)(1) ("Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent"), https://www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=16:1.0.1.3.36#se16.1.312_12.

make reasonable efforts to verify that consent is given or authorised by the HPR over the child, taking into consideration the available technology.

The FTC has approved the use of several methods to ensure that the person giving the consent is the child's parent. These include:

- Signing a consent form and sending it back via electronic scan, mail or fax;
- Using a credit card, debit card or other online payment system that provides notification of each separate transaction to the account holder;
- Calling a telephone number staffed by trained personnel for free;
- Connecting to trained personnel via video conference;
- Providing a copy of a form of government-issued ID that the ISS checks against a database, as long as the ISS deletes the identification from its records when it finishes the verification process;
- Answering a series of knowledge-based challenge questions that would be difficult for someone other than the parent to answer;
- Verifying a picture of a driver's license of other photo ID submitted by the parent and then comparing that photo to a second photo submitted by the parent, using facial recognition technology; or
- Using a consent method known as "email plus". In lower-risk situations where a child's personal data is used by an ISS only for internal purposes and will not be disclosed, the FTC permits use of "email plus," by which the ISS obtains consent via email, accompanied by a follow-up confirmation to the parent.[20]

These methods could provide an acceptable basis for verifying parental consent has been given under the GDPR for both low- and high-risk scenarios. It would be helpful to review the relationship between COPPA requirements for a neutral parental verification mechanism and GDPR data minimisation requirements.

Additionally, these are not the only methods that could work under the GDPR and the development of new and innovative verification mechanisms is encouraged.

[20] See US Federal Trade Commission, "Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business", https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance.

Furthermore, while verifying consent is given or authorised by an adult alone is not enough to meet the requirements of Article 8(2), controllers should not design mechanisms in a way that requires excessive amounts of data collection to prove that the adult who gave or authorised the consent is in fact the HPR. Rather, there must be flexibility for industry to develop different solutions depending on the context of the processing and the level of risk involved. For instance, requiring the provision of a child's birth certificate and a parent's government issued ID is far too excessive and goes against principles of data minimisation. Indeed, the WP29, in its consent guidelines, notes that it is up to the controller to determine what measures are appropriate in a specific case and that as a general rule, controllers should avoid verification solutions which themselves involve excessive collection of personal data.[21]

Finally, it would be desirable for supervisory authorities to work together and with industry to agree on acceptable parental consent mechanisms that are effective and reliable.

IX. Expiration of Parental Consent

The WP29 states, on pages 26 and 27 of its consent guidelines, that consent obtained from a parent expires automatically when a child reaches the age of digital consent and that the consent must then "be reaffirmed by the data subject personally". The ICO Consultation also states that, if a controller relies on parental consent while the child is under the age of digital consent then the controller must obtain the child's own consent once the child reaches the relevant age.

The GDPR does not require that consent expires upon reaching the age of digital consent. As previously noted, questions of children's competence are generally matters of Member State law. Article 8 is silent on the issue so it must be assumed that the WP29 and the ICO consider that this same requirement would apply to any consent given by an HPR in respect of processing carried out when a child was not able to give his or her own consent. This has never been suggested under previous data protection provisions and there is no authority for it in the GDPR. Parents provide consent on behalf of their children for a multitude of processing activities, from doctors to sports clubs, from schools to holiday companies. A requirement for a child to actively reaffirm consent for all the processing by all the controllers who process personal data on them once the child reaches the age to give an independent consent would be a huge and unnecessary burden and would disregard instances where the parent authorised the child's consent.

In practical terms, in the case of ISS providers, it would present significant challenges as it requires a controller to know and retain information on the country and age of the child so that a request for reaffirmation of consent may be presented in time. Some services are deliberately architected to preclude access to such user data for privacy purposes. In many instances,

[21] See footnote 2 at page 26.

requiring this type of tracking to comply with Article 8 would require the collection of specific age data.

It also causes potential problems where families move between Member States that vary in their age of digital consent. For example, if parental consent is obtained when a child, who is aged 14, is in a country where the age of digital consent is 16 and then the child moves to a country where the age threshold is 13, the provider may not have collected the information to know that they need the child's direct consent as the parental consent will no longer apply.

The GDPR provides that consent be "given or authorised by the HPR". Consent is given on behalf of a child when he or she is under the age of digital consent. In such cases, it can be presumed that the consent endures for the benefit of the child even after he or she has attained the age of digital consent. If this were not the case, the child would be deprived of the service to which the HPR has consented on his or her behalf. Additionally, a child who has reached the age of digital consent, where consent was given by a parent, would have information about their right to withdraw consent available to them via a privacy policy or other privacy tools or dashboards and could exercise this right should they wish to do so.

If the parent initially authorises the child herself or himself to consent and has acted to help effectuate the child's own privacy choices, then that parentally authorised consent by the child should continue to apply when the child attains the applicable digital age of consent. This makes even more sense because the child in this case may have taken active steps to give the consent after receiving authorisation from the HPR and so is more involved and clearly requesting the processing. Additionally, the child who has reached the age of digital consent could simply withdraw consent if they no longer wish for the ISS to process their personal data.

In summary, where a HPR gives or authorises consent for processing a child's personal data under Article 8(1), such consent remains valid when the child attains the age of digital consent, unless: (i) the child or parent withdraws consent before then; (ii) the child withdraws consent when they reach the age of digital consent; (iii) the ISS becomes aware that the consent was not valid because it was not given in the child's best interests.

X. Transparency and Age Appropriate Notices

Transparency, an essential element of accountability, is an intrinsic part of any consent and a key requirement under the GDPR. Article 12 specifically references children and provides that the controller shall take appropriate measures to provide the individual with information required by the GDPR in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

Although transparency is essential to ensuring consent is informed, the requirements extend to several areas of the GDPR. With respect to children, several important issues arise, including:

- For processing based on legitimate interest, how should organisations communicate the controller's legitimate interests to a child?

- How can organisations notify children about personal data breaches if they are among those affected by a breach?

- For processing based on consent, how can organisations appropriately construct notices which are intelligible to children?

CIPL believes that multiple notices are undesirable. For organisations that put in place two versions of a notice (a standard notice and a child-friendly notice) there can be serious consequences if the notice becomes the subject of an enforcement action and questions arise as to which text is controlling. Such an issue may arise as there is the potential for certain information to become lost in translation when converting an adult notice to a child-friendly notice.

A more appropriate approach is to consider the services' audience. Providers of services directed to adults only, by the nature of their content and context, should be able to provide standard notices intelligible to adults. Providing notice to children as to why they are not allowed to use the service, in language they can understand, is a good practice that organisations can employ if their service is directed to adults only. Services directed to children should provide notices intelligible to children. This is not limited to textual notices, as audio and video notices may be effective for children who have not yet developed the capacity to read.

The situation is less clear when dealing with a mixed audience service (i.e. if the service is not directed to children but children nonetheless use the service). For processing based on consent and within the scope of Article 8, notices need only be intelligible to children aged 13 years and older as parental consent is required for children below this age threshold.[22] For such services, as a best practice, child-friendly learning notices designed to familiarise young children with the concept of consent may be employed but this is not required.[23] Parents, on the other hand, should be given an opportunity to view the privacy notice as part of the parental verification mechanism. For processing based on consent outside the scope of Article 8 or processing based on other grounds, the notice must be intelligible to children of the relevant ages.

Traditionally, privacy notices have been long, complex and full of legal terminology unintelligible to the general public. The GDPR's requirement to provide information in a

[22] CIPL acknowledges this may be higher depending on the Member State in question but ensuring children aged 13 and over can understand such notices ensures children in all Member States interacting with the service are covered.

[23] A "learning notice" should be labelled as such to make clear that it is an educational tool and does not affect in any way or displace the legal effect of the actual privacy notice. In enforcement actions, the privacy notice will control and the learning notice shall have no effect.

concise, transparent, intelligible and easily accessible form, using clear and plain language, has resulted in a shift in outlook, by both organisations and regulators, in how appropriate notice should be provided. For instance, the WP29 has endorsed the use of layered notices in its recent guidelines on consent and transparency.

To date, notices have not been specifically written for or targeted at children. Summary notices have been used by some organisations to provide more accessible language, but there is no standard for appropriate notices to very young children. Organisations should be permitted to design notices they think are the most appropriate to cater to the general audience, taking into account that the audience may include young children.

Regarding security breach notices, the notice should be intelligible to children of all ages. One possible safeguard could be to provide an additional statement upfront in the notice that if the reader is under 18, to show the notification to their parent or guardian before resuming use of the service, as it contains important information.

XI. Marketing to Children

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.[24] 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 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.[25]

[24] 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/).

[25] 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.

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.

XII. Automated Decision-Making, Including Profiling, Regarding Children

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 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.[26]

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

[26] See footnote 3 at page 28.

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.[27] 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.

XIII. National Age Thresholds and the Lead Supervisory Authority

Important questions arise around how age thresholds under Article 8 relate to the territorial scope of national laws implementing the GDPR and to the competence of the (lead) DPA. CIPL notes the following points:

[27] For a full discussion of CIPL's position in relation to what types of automated decisions do and do not produce legal or similarly significant effects, see CIPL's comments to the WP29 Guidelines on Automated Individual Decision-Making and Profiling, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_to_wp29_guidelines_on_automated_individual_decision-making_and_profiling.pdf.

- Member States take different approaches as to the territorial scope of their national implementing laws. In some Member States, the scope is based on the establishment of the data controller while in others it is based on the effect of a processing activity on individuals residing within their own Member States. The Netherlands is a clear example of the first approach and France of the second approach[28];

- In cross-border situations, the competence of each national DPA will be replaced by the competence of a lead DPA and cooperation through the one-stop-shop mechanism. However, in some situations, each national DPA may be mandated to handle complaints lodged with it (see Article 56 GDPR);

- The GDPR defines cross-border processing in Article 4(23) but this definition does not necessarily provide clarity on the application of Article 8;

- In cross-border situations, a lead DPA may be required to apply the national law of another Member State;

- Of course, many of these problems would be solved if all Member States adopted the same digital age of consent threshold. However, this seems unlikely in view of the state of the draft implementing laws.

To illustrate the relevance of these issues, there is no uniformity in the EU as to which age threshold applies where:

- A controller has one main establishment but offers services to children in multiple Member States;

- A child is usually resident in one Member State but moves temporarily to another;

- A child is usually resident in one Member State but moves permanently to another.

In the absence of specific criteria under the GDPR, each Member State makes its own assessment. Several factors could be considered, each presenting different challenges.

Firstly, a Member State could consider the place of establishment. In this case, the age threshold that applies is that of the Member State where the controller is established. The effect of this would be that a child resident in another Member State with a higher age threshold for digital consent would be permitted to use the service if they have attained the age of digital consent in the Member State where the controller is established. This raises a

[28] The GDPR does not contain any provisions on applicable national law in situation where a controller has an EU establishment. There is a reference in Recital 153, but this is specifically linked to Article 85 GDPR (processing for journalistic purposes).

question around organisations deliberately establishing themselves in Member States with a 13 year age threshold to permit children of all Member States to use the service and renders pointless the margin of manoeuvre for Member States to set their own age.

Secondly, the determining criterion could be a child's place of residence. In this case, the age threshold that will apply is that where the child is resident. This scenario is potentially more complicated as controllers will need to ascertain the age of each child user to determine whether they are above or below the age of digital consent and, as a result, whether consent of the HPR must be given or authorised. Even more complexity is added in the case of children temporarily moving between Member States (for example for summer holidays).

The WP29 and ICO seem to acknowledge this complexity. The WP29 states that controllers providing cross-border services cannot always rely on complying with only the law of the Member State in which it has its main establishment. This view is also contained in the ICO guidance on the basis that the law which applies to the processing is the law of the Member State where the child is resident. The ICO considers that if a service is offered to users outside the jurisdiction from which the service is run it may be necessary to check the age of visitors in relation to the age of consent in the target country.

Although determining the applicable law and competent DPA on the basis of a child's place of residence is the approach suggested by the WP29 and the ICO,[29] CIPL wishes to underline the consequences of this approach for the digital internal market. Such an approach would compel service providers to modulate their services in each Member State. Although DPAs do not define the territorial scope of national implementing laws, they should draw attention to this issue and highlight the importance of a consistent approach. This is particularly relevant at present as most national governments and parliaments are finalising national data protection laws. DPAs should also highlight this issue to the European Commission. Additionally, DPAs should consider the complexity of this issue when carrying out their enforcement duties.

With regard to the competence of the lead supervisory authority, Article 4(23) on the definition of "cross-border processing" states that if processing in the context of the establishment of the controller substantially affects individuals in another Member State, it falls within the definition of cross-border processing. For such cases, a lead DPA would be competent and the one-stop-shop mechanism would be applied.

In this specific context, we point to Article 56(2) GDPR which contains a derogation that could be applied in case an individual complaint concerns a particular child in a specific Member State; therefore it could be a matter for the national supervisory authority in that Member State. CIPL, however, takes the view that all processing which involves a systemic business

[29] See footnote 2 at page 24-25 and footnote 4 at page 28 (Document unnumbered but page 28 appears under the Section "What are the rules about an ISS (online service) and consent?").

process should be handled by the lead DPA under the one-stop-shop mechanism. Article 56(3) GDPR makes this possible. We suggest that this preference be included in future EDPB guidance.

Finally, this section highlights the difficulties of having multiple age thresholds among the Member States. Harmonisation is a key goal of the GDPR and CIPL is of the view that Member States should carefully review their draft GDPR bills before they are finalised and reconsider their age thresholds to be in line with those of other Member States.

XIV. Exercise of Rights by Children

The GDPR does not mandate an age threshold in respect of children exercising their GDPR rights on their own. This is a separate question from whether a child is able to consent to data processing under Article 8. For example, Article 17 is silent on the age at which an individual can exercise his or her right of erasure.

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". [30]

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[31] 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.

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

[30] UK ICO, Subject Access Request, https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/subject-access-request/.
[31] See footnote 1.

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 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.

XV. Dealing with Existing Users

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. Given that the majority of Member States have not yet finalised their national law specifying the age of digital consent, controllers have no choice but to wait in order to start the implementation of Article 8.

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.