Deloitte.

Fundamentals:
A Guide to Protecting Children's Personal Data

Deloitte Ireland, Data Privacy Services

About a quarter of Ireland's population are children, all of whose personal data is processed every day online and offline, in educational, health, recreational and sporting, social services, and commercial contexts. Children's data protection is one of the Irish Government's priorities and has been a key focus for the Irish Data Protection Regulator. This is leading to new legislation and increased regulatory scrutiny.

In December 2021, following extensive public consultation, the Irish Data Protection Commission (the **"DPC"**) launched a comprehensive guidance entitled "Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing" (the **"Fundamentals"**). The General Data Protection Regulation (the **"GDPR"**) recognises the specific circumstances and risks posed to children when their personal data is collected and processed without adequate safeguards. The Fundamentals introduce child-specific data protection interpretative principles and recommended measures that will enhance the level of protection afforded to children against the data processing risks posed to them by their use of/access to services in both an online and offline world.

What are the DPC's Fundamentals?

14 key principles are set out for organisations to follow when processing children's personal data:

1. Floor of protection: Online service providers should provide a "floor" of protection for all users, unless they take a risk-based approach to verifying the age of their users, so that the protections set out in these Fundamentals are applied to all processing of children's data.

2. Clear-cut consent: When a child has given consent for their data to be processed, that consent must be freely given, specific, informed and unambiguous, made by way of a clear statement or affirmative action.

3. Zero interference: Online service providers processing children's data should ensure that the pursuit of legitimate interests do not interfere with, conflict or negatively impact, at any level, the best interests of the child.

The Fundamentals are a code of practice for protecting children's personal data in Ireland. The final version was published by the DPC on 17th December 2021, with immediate application and operational effect in forming the basis for the DPC's approach to supervision, regulation and enforcement in the area of processing of children's personal data.

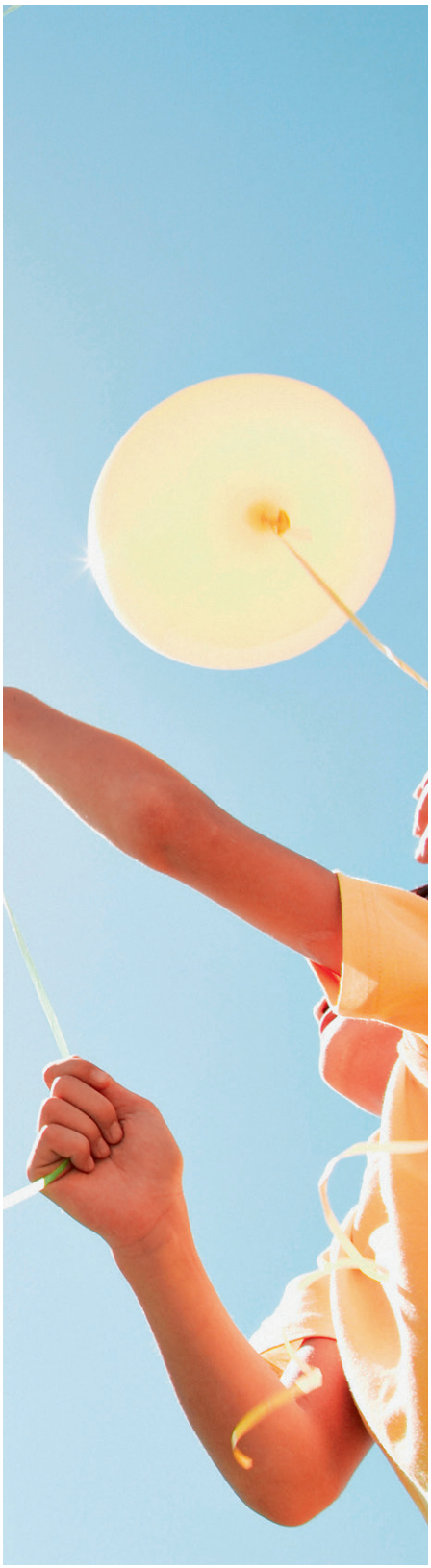
4. Know your audience: Online service providers should take steps to identify their users and ensure that services directed at, intended for or likely to be accessed by children have child-specific data protection measures in place.

5. Information in every instance: Children are entitled to receive information about the processing of their own personal data irrespective of the legal basis relied on and even if consent was given by a parent on their behalf to the processing of their personal data.

6. Child-oriented transparency: Privacy information about how personal data is used must be provided in a concise, transparent, intelligible and accessible way, using clear and plain language that is comprehensible and suited to the age of the child.

7. Let children have their say: Online service providers shouldn't forget that children are data subjects in their own right and have rights in relation to their personal data. The DPC considers that a child may exercise these rights at any time as long as they have the capacity to do so and it is in their best interests.

8. Consent doesn't change childhood: Consent obtained from children or from their guardians/ parents should not be used as a justification to treat children of all ages as if they were adults.



9. Your platform, your responsibility: Companies who derive revenue from providing or selling services through digital and online technologies pose particular risks to the rights and freedoms of children. Where such a company uses age verification and/or relies on parental consent for processing, the DPC will expect it to go the extra mile in proving that its measures around age verification and the verification of parental consent are effective.

10. Don't shut out child users or downgrade their experience: If a service is directed at, intended for, or likely to be accessed by children, you can't bypass your obligations simply by shutting them out or depriving them of a rich service experience.

11. Minimum user ages aren't an excuse: Theoretical user age thresholds for accessing services don't displace the obligations of organisations to comply with the controller obligations under the GDPR and the standards and expectations set out in these Fundamentals where "underage" users are concerned.

12. A precautionary approach to profiling: Online service providers should not profile children and/or carry out automated decision making in relation to children, or otherwise use their personal data, for marketing/advertising purposes, due to their particular vulnerability and susceptibility to behavioural advertising, unless they can clearly demonstrate how and why it is in the best interests of the child to do so.

13. Do a DPIA: Online service providers should undertake data protection impact assessments ("DPIA") to minimise the data protection risks of their services, and in particular the specific risks to children which arise from the processing of their data. The principle of the best interests of the child must be a key criterion in any DPIA and must prevail over the commercial interests of an organisation in the event of a conflict between the two sets of interests.

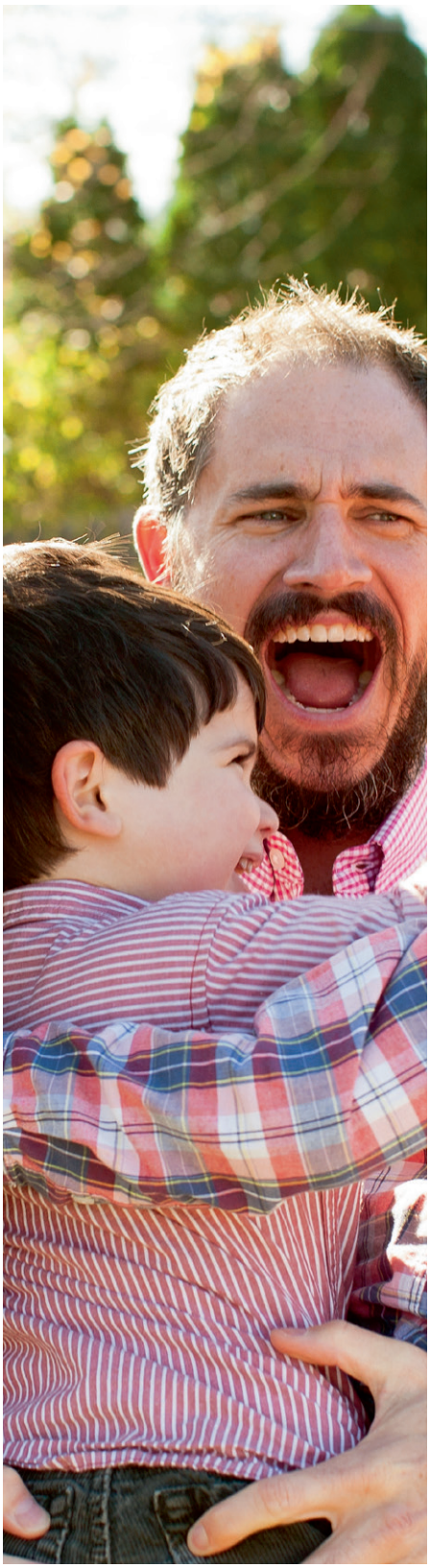
14. Bake it in: Online service providers that routinely process children's data should, by design and by default, have a consistently high level of data protection which is "baked in" across their services.

With regard to obligations under the GDPR, it is important for organisations to recognise that children may be less aware of the risks, consequences and safeguards involved when their personal data is processed. They may also not be aware of their data protection rights. A child's age, maturity and development capacity will also impact their ability to understand and mitigate risk. The Fundamentals set the marker for organisations that process children's data by establishing the baseline expectations of the DPC as the regulator for the processing of children's data in Ireland. Organisations should know their users/audience and have knowledge about the people they collect information from. They should assess whether a website, application or other online service is likely to be accessed by children.

The 'Best Interest' Principle

The best interests of the child are paramount when considering the position of children as data subjects. This often means balancing the 'protection' factors requiring restriction of access against 'empowerment' factors that allow children to access appropriate online services.

The age and development capacity of the child should also be taken into account. Organisations must be able to demonstrate that the 'best interest' principle has been given due consideration as part of the overall Data Protection Impact Assessment (DPIA) process.



What are the risks to children

Processing children's personal data online and offline could put children's privacy and the rights and freedoms afforded to them under the GDPR, amongst other laws, at risk. We see scenarios where a child is shown inappropriate advertisements or content online; a child's data is collected without valid consent or shared with a third party who then uses the data in an unwarranted manner; or a child is profiled as part of a non-essential service and the child is unaware of how, why or when the profiling takes place.

It is crucial to protect children's privacy and drive compliance with the Fundamentals. Privacy awareness amongst the general public, consumers and customers is rising at a rapid rate. In addition to their legal obligations, organisations should consider and address these societal concerns to build trust and maintain reputation. There is also a commercial element to using personal data in a fair and transparent way, where baking children's privacy into products can increase the effectiveness and value of new revenue streams.

What services are considered in-scope?

A service that is directed at, intended for, or likely to be accessed by a child under the age of 18 years. Offline data processing is also in-scope, this applies to educational providers, sports and social clubs, health and social support providers amongst others.

The Fundamentals will lead to changes in practice for major industries such as media, telecoms, entertainment, hospitality, transportation, retail, and technology. Examples of in-scope services include but are not limited to:

- A streaming service where children can watch videos or listen to music that is personalised to them
- A social media platform that allows children to interact, upload and share experiences
- A multi-platform gaming service where children can play together online
- A restaurant that provides a membership scheme that can accessed online to view loyalty points, discounts, and orders
- A transport provider's mobile app that allows users to book travel and offers a discount scheme to children
- A primary school's data systems recording children's school activity

What should organisations consider when it comes to applying the Fundamentals to operations

When offering a service that is directed at, intended for, or likely to be access by children, organisations should give due consideration to the following:

• **Consent:** If consent is being relied on to process children's data, it must be freely given, specific, informed and unambiguous. Organisations should ensure that the child is given a real choice over how their personal data is used and that they have the capacity to understand exactly what they are consenting to. It is also important to consider the 'digital age of consent', which is the minimum age at which online service providers can rely on a child's own consent to process their data, in Ireland this is 16 years of age.

• **Transparency:** The GDPR requires that individuals must be given certain key pieces of information about the use of their personal data by an organisation. It is vital that organisations know their audience so that they can tailor their transparency information and notifications to ensure they can be understood as readily by a child as by an adult.

• **Data Subject Access Rights (DSARs):** Organisations should be mindful of access rights. Large-scale online platforms and digital service providers will likely rely upon automated tools for the purpose of enabling data subjects to exercise their data protection rights. Organisations should have a dedicated, clear and child-friendly user flow in place to facilitate children exercising their rights. They should consider the circumstances where exceptions may arise which would call for individual assessments (non-automated/human involvement). If a child is under 16 and parent/guardian consent was required for the online service provider to process the child's data, it follows that they should be able to exercise the access rights but only if it is in the best interest of the child to do so.

• **Age verification:** The degree of certainty to be established by online providers that consent has been given by the holder of parental responsibility, in line with obligations under the GDPR, is that the organisation must make 'reasonable efforts' to verify this 'taking into consideration available technology'. Digital consent obtained from children over the age of digital consent or from guardians/parents of children under the age of digital consent, should not be used as a route to treat children of all ages as if they were adults. It acts as a marker for online services to consider the nature and design of their services, and how to make them age appropriate for their users. For technology and internet companies with a vast array of available digital and online technologies and the higher risks to data subjects who utilise their platforms, this places a higher burden on organisations in their effort to both verify age and verify that consent has been given by the parent/guardian of a child user.

• **Don't lock children out:** The provision of a two-tier approach, with an inferior level of central services and features offered to children, risks depriving children of their full rights. It also risks driving children underground. This can be counter-productive on an organisation's part in that it may result in child users circumventing age verification measures and accessing a service that does not adhere to the highest levels of data protection. High levels of data protection by design and default also ensure that children are not targeted with age-inappropriate content.

- **Direct marketing, profiling and advertising:**
  - The GDPR does not impose an outright ban on organisations marketing to children but it does require that there be specific protections for children when marketing to them or creating user profiles. Electronic direct marketing is governed in the first instance by the ePrivacy Regulations. If an organisation engages in the sending of electronic direct marketing, it needs the affirmative consent of the individuals it wishes to send those messages to. This requirement applies regardless of whether the material is being sent to an adult or child. A person must be able to withdraw consent and there must be a valid means to allow them opt-out free of charge. Consent to the receipt of electronic direct marketing messages can only be provided by a child who is over the age of 16 (digital age of consent) or by a parent/guardian of a child who is under 16.

  - Where a product or service uses cookies, the organisation should conduct audits to establish how these cookies might be used to profile individuals and they should have particular regard for how children may be targeted as a result of their use. A user interface seeking cookies consent from children should provide clear and comprehensible information written in a child-friendly way to explain what cookies do and how the information obtained will be used, and by what other organisations.

  - It is the DPC's position that organisations should not profile children, engage in automated decision-making concerning children, or otherwise use their personal data, for advertising/marketing purposes, unless they can clearly demonstrate how and why it is in the best interests of children to do so.

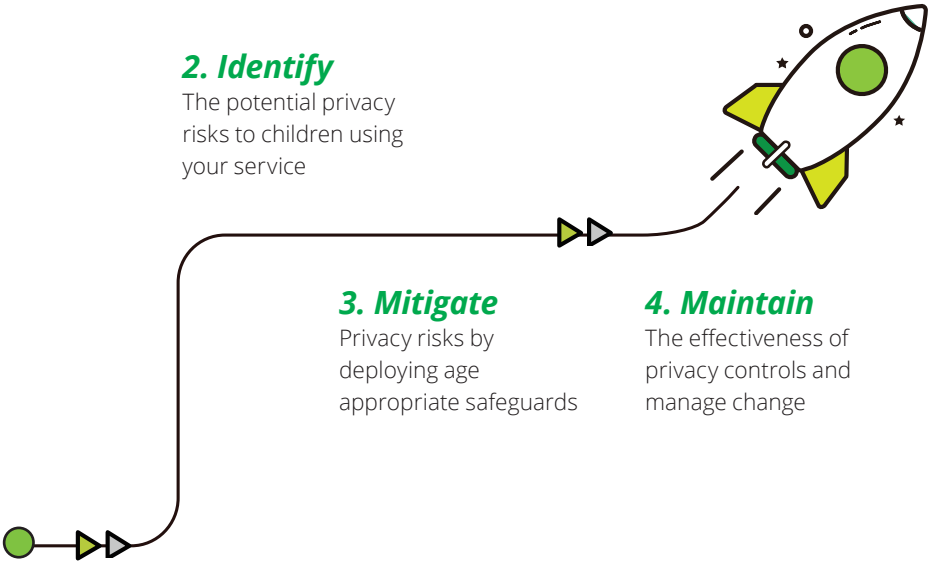
  - Profiling may pose a risk to the ability of children to independently form their own opinions and make decisions, given that profiling for the purposes of personalising information society services can influence the information or content presented to them. Organisations must ensure that profiling does not encroach upon children's free will and their capacity to make autonomous decisions and does not restrict their right to access appropriate information from a wide range of national and international sources.

  - The DPC has identified that a DPIA will be mandatory for processing operations involving 'profiling vulnerable persons including children to target marketing or online services at such persons. A child-orientated DPIA is the first step in mitigating risk arising from processing children's personal data and will be seen as a key act of compliance. Organisations should consider conducting Child Rights Impact Assessments (CRIA), which is a child-focused human rights impact assessment that uses UNCRC (UN Convention on the Rights of the Child) as its framework.

- **Key actions for organisations to consider:**
  - Map what personal data you collect from children
  - Check the age of the users interacting with your online/offline services
  - Recognise children have the right to exercise their data protection rights to access, erasure and restriction of processing independently of their parents, where appropriate
  - Switch off non-essential profiling for advertising purposes
  - Turning off geolocation services that track where in the world your visitors are
  - Don't use nudge techniques to encourage children to provide more personal data
  - Provide a high level of privacy by design and default

How can Deloitte help?

Deloitte's age-appropriate privacy design framework is a pragmatic, risk-based approach that can be followed to build trust, enhance user experience and demonstrate compliance with the DPC's Fundamentals. Following a 4-step approach, we can work with you to design, implement and maintain privacy controls to align to the 14 Fundamentals.



1. Understand
Where and how you process children's data online and offline

2. Identify
The potential privacy risks to children using your service

3. Mitigate
Privacy risks by deploying age appropriate safeguards

4. Maintain
The effectiveness of privacy controls and manage change

Contact us:

Colm McDonnell
Partner
Risk Advisory
Tel: +353 1 417 2348
Email: cmcdonnell@deloitte.ie

Nicola Flannery
Director
Risk Advisory
Tel: +353 1 417 2665
Email: niflannery@deloitte.ie

Laura Skelton
Senior Manager
Risk Advisory
Tel: +353 1 417 3875
Email: laskelton@deloitte.ie

Deloitte.

Designed by CoRe Creative Services. RITM1015475