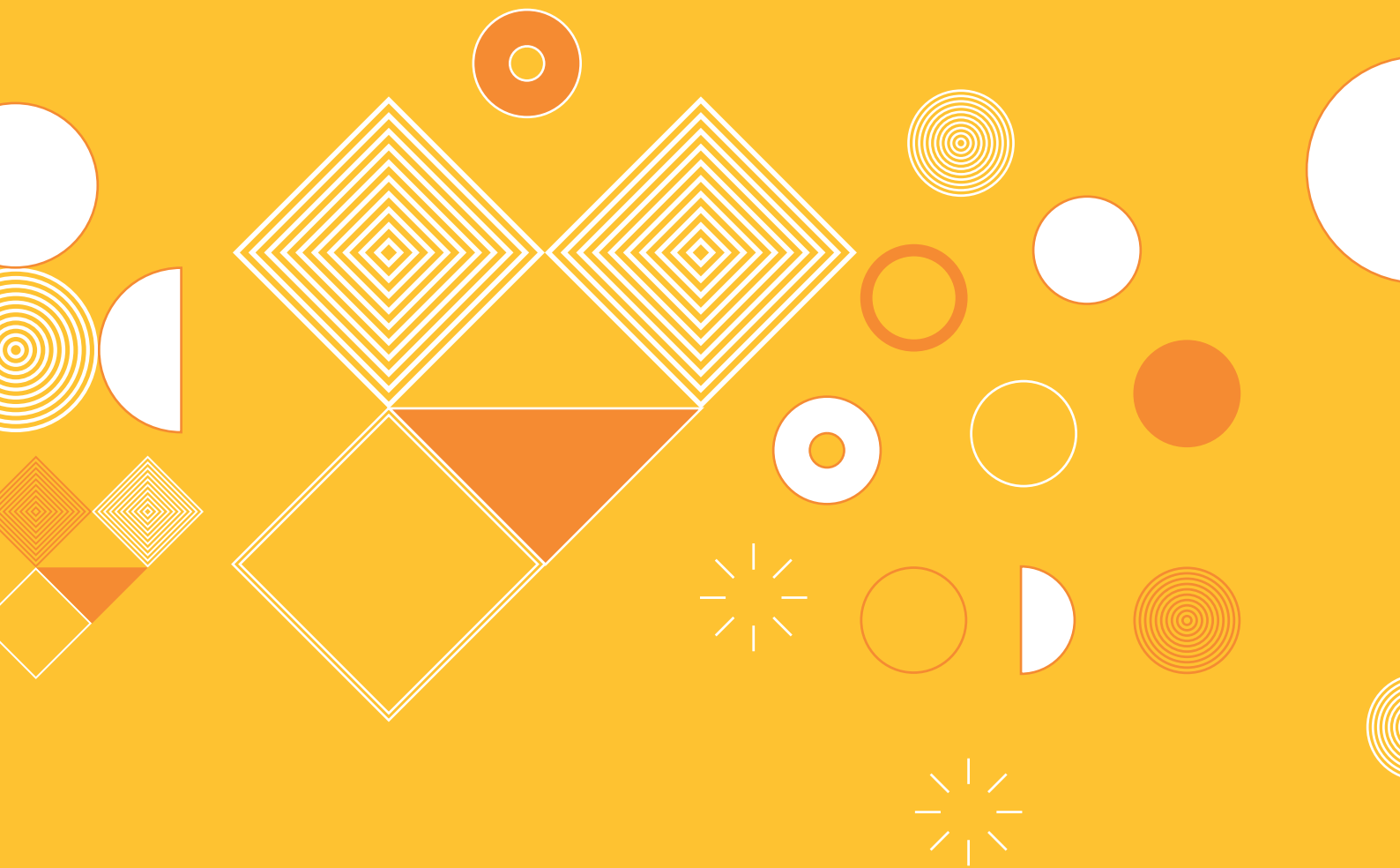


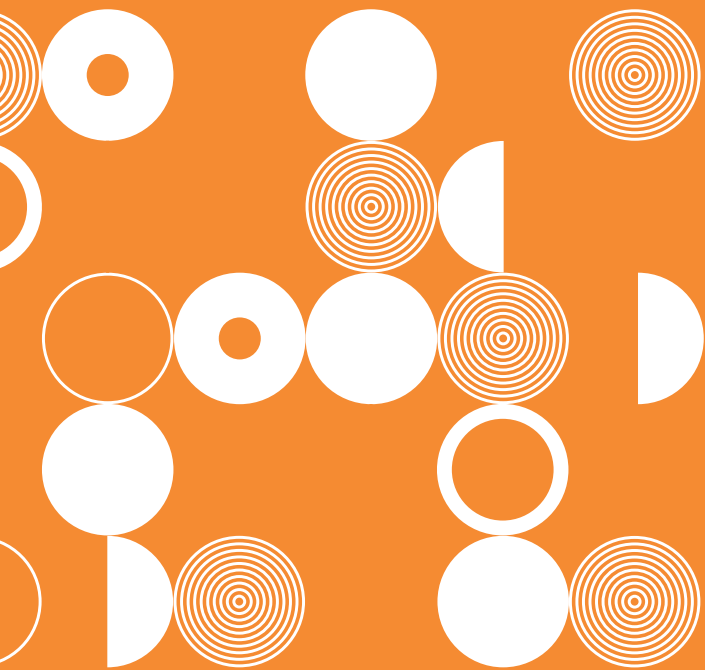
Data Protection Commission

Public consultation on the
processing of children's
personal data and the rights
of children as data subjects
under the General Data
Protection Regulation




An Coimisiún um
Chosaint Sonraí
Data Protection
Commission


LAUNCHED 19 DECEMBER 2018
DATA PROTECTION COMMISSION,
21 FITZWILLIAM SQUARE, DUBLIN 2

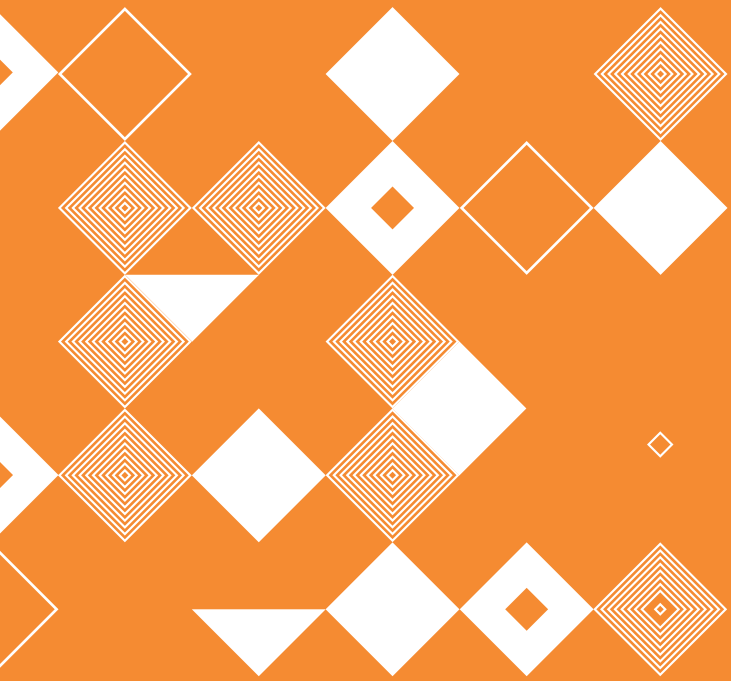


Contents



Introduction	4
What is data protection?	5
What is personal data?	5
What does “processing” mean?	5
What is the General Data Protection Regulation?	5
Rights and obligations	6
What are data protection rights?	7
Children’s rights under the GDPR	7
The DPC’s obligations under the GDPR and the Data Protection Act 2018	8
Format of the DPC’s public consultation	8
Objective of the consultation	9
Questions for public consultation	10
I. Children as data subjects and the exercise of their data protection rights	11
(A) Transparency and the right to be informed about use of personal data (Articles 12-14 GDPR)	11
(B) Right of access (Article 15 GDPR)	11
(C) Right to erasure (“Right to be forgotten” – Article 17 GDPR)	12
II. Safeguards	13
(A) Age verification (Article 8 GDPR)	13
(B) Online service providers and different national ages of digital consent in the EU (Article 8 GDPR)	14
III. Profiling and marketing activities concerning children (Articles 21-22 GDPR)	14
IV. Data protection by design and by default (Article 25 GDPR)	15
V. General	15





Introduction



WHAT IS DATA PROTECTION?

Data protection law is about everyone's fundamental right to the protection of their personal data. When you give your personal data to an organisation, they have a duty to comply with certain rules which limit what they can do with your personal data. Collectively, these rules, together with the rights that someone has to protect their personal data, are known as data protection. Organisations that decide on why and how to use your personal data are known in data protection law as "data controllers", while people who give their personal data to organisations are called "data subjects".

WHAT IS PERSONAL DATA?

Personal data is any information that relates to you personally or would identify you. In other words, it is any piece of information that helps someone to know who you are, such as your full name, your date of birth, your email address, your phone number, or your address, for example.

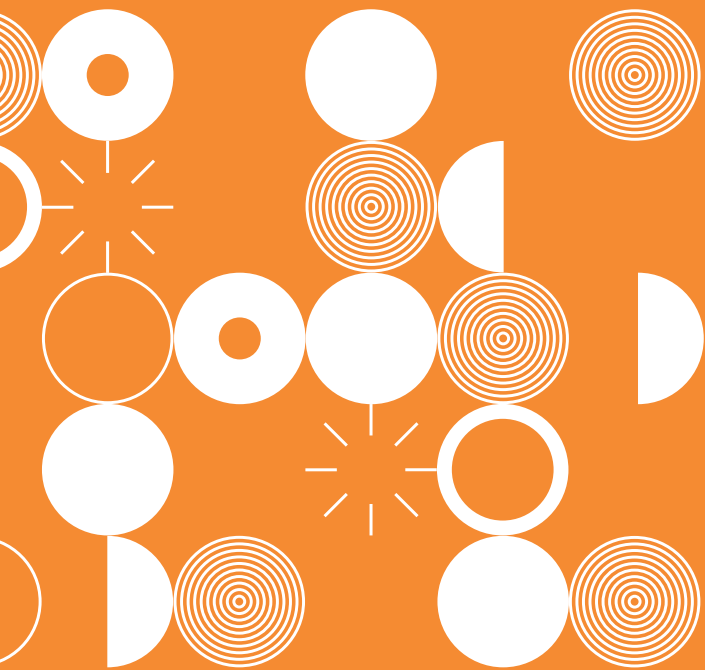
WHAT DOES "PROCESSING" MEAN?

Data protection law sets out the rules that apply to the processing of personal data by organisations. Processing basically means using personal data and doing anything with it, from collecting to storing it, retrieving it, consulting it, sharing it with someone else, erasing it and destroying it.

WHAT IS THE GENERAL DATA PROTECTION REGULATION?

The General Data Protection Regulation (GDPR) is an EU law which came into force on 25 May 2018. It is essentially a new set of data protection rules concerned with ensuring that each of us knows when personal information about us is collected and how it will be used, and giving us more control over the use of this personal data. One of the many changes the GDPR has brought about is the new emphasis placed on the importance of the protection of children's personal data. Before the GDPR, there was no mention of children at all under the old EU data protection law. Now, the GDPR says that children merit specific protection when it comes to the processing of their personal data because they may be less aware of the risks, consequences and safeguards involved as well as their data protection rights.

The introduction of the GDPR means that, for the first time, there is now an EU data protection law in place that devotes special attention to the protection of personal data of children and the position of children as data subjects. However, as the GDPR is a principles-based law, questions arise about how a number of GDPR provisions in this area should be interpreted and implemented in practice.



Rights & obligations



WHAT ARE DATA PROTECTION RIGHTS?

Individuals have specific rights in relation to their personal data. These rights include, amongst others:

- (i) the right to be informed about who holds your personal data and why it is being processed (transparency),
- (ii) the right to access and be given a copy of your personal data (access),
- (iii) the right to rectify inaccurate or incomplete personal data (rectification), and
- (iv) the right to have your data erased (erasure).

CHILDREN'S RIGHTS UNDER THE GDPR

There tends to be a general misconception that children do not have the same data protection rights as adults, but this is not the case. Children have all of the same rights as adults over their personal data – data about them is still their personal data and does not belong to anyone else, such as a parent or guardian. However, one of the issues the GDPR does not address is when children should be able to exercise these rights for themselves. In Ireland, for data protection purposes, a child is somebody under the age 18.

Data protection rights apply to children just as much as they do to adults. However, there are child-specific protections attached to some of these provisions, which organisations must take into account. For example, organisations have an express obligation under the GDPR to ensure that any transparency information about data processing which is addressed to a child should be in clear and plain language so that the child can understand it (Article 12.1).

Article 8 of the GDPR (commonly referred to as the “age of digital consent”) sets the limitations as to the minimum age at which online service providers can rely on a child’s own consent to process their personal data. In Ireland, the Data Protection Act 2018 gives further effect to the GDPR and has set the age of digital consent at 16, which means that if an organisation is relying on consent as the legal basis (justification) for processing a child’s personal data and the child is under 16, then consent must be given or authorised by the person who has parental responsibility for the child.



THE DPC'S OBLIGATIONS UNDER THE GDPR AND THE DATA PROTECTION ACT 2018


Article 57 of the GDPR states that data protection authorities like the DPC have an obligation to promote public awareness and understanding of the risks, rules, safeguards and rights in relation to the processing of personal data, especially the processing of personal data relating to children. Additionally, under the Data Protection Act 2018, which gives further effect to the GDPR in Ireland, the DPC has an obligation under Section 32 to encourage the drawing up of codes of conduct in relation to certain issues concerning the processing of children's personal data. The DPC has launched this public consultation to give all stakeholders an opportunity to have their say on issues around the processing of children's personal data, the specific standards of data protection applicable to children, and the rights of children as data subjects. The DPC invites responses from all interested parties, including, amongst others, parents, educators, organisations that represent children's rights, child protection organisations, representative bodies for parents and educators, as well as organisations that collect and process children's data.

However, the DPC also wants to give children and young people an opportunity to have their say too. The UN Convention on the Rights of the Child makes it clear that children have the right to express their views freely in all matters affecting them, with due weight given to their views according to their age and maturity.

FORMAT OF THE DPC'S PUBLIC CONSULTATION

For that reason, there are two streams to the DPC's public consultation on children and data protection issues – one aimed at adult stakeholders, and the other aimed directly at children and young people.

This document is the adult-centred stream of the consultation. However, in January 2019, the DPC will also launch its special consultation directly with children and young people by inviting all schools and Youthreach centres in Ireland to participate in that consultation. The DPC has created a lesson plan on personal data and data protection rights which will help teachers to teach their students about basic data protection rights and allow them to collect the opinions and views of their students on these important areas and feed this back to the DPC in a way that does not identify any particular student. This lesson plan will be sent directly to all schools and Youthreach centres in Ireland and will also be available publicly on the DPC's website at the end of January 2019.



Involving children and young people directly in this consultation will be a challenge for the DPC as many concepts in data protection can be difficult for any of us to understand, even for those of us in the DPC and for data protection practitioners. It can also be challenging to separate out data protection and privacy issues from other issues and risks that present for children when they are active online, such as cyberbullying, online addiction, and harmful content. Bearing in mind the DPC's statutory remit as the regulator and enforcer for data protection issues, this consultation will focus solely on *data-protection-specific* issues.

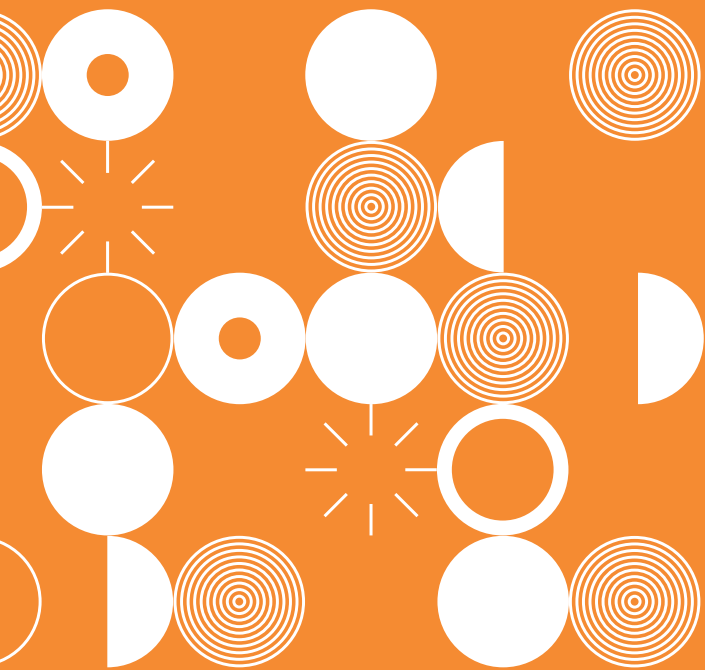
OBJECTIVE OF THE CONSULTATION

The DPC will use the responses¹ from both streams of its consultation to produce guidance materials, which will include guidance specifically for children and young people, as well as guidance for organisations who process the personal data of children and young people. In addition, following the consultation, the DPC will also work with industry, government and voluntary sector stakeholders and their representative bodies to encourage the drawing up of codes of conduct to promote best practices by organisations that process the personal data of children and young people.

This stream of the consultation will be open for responses from all interested parties from 19 December 2018 until 1 March 2019 inclusive. Parties making submissions should feel free to respond to any or all of the questions set out below. Submissions should be emailed to childrensconsultation@dataprotection.ie.

It should be noted that the DPC intends to publish on its website the content of all submissions received as part of this stream of the consultation and the identity of the party making the submission (unless that party is an individual and has expressly requested not to be so identified).

1. While the DPC will consider all responses received by it, there should be no expectation by any party making a submission to the DPC that any issue, position or view raised in that submission during this consultation will be addressed in any new or updated GDPR guidelines that may be produced by the DPC.



Questions



QUESTIONS FOR PUBLIC CONSULTATION

The DPC seeks submissions in response to the questions set out in respect of each of the following issues:

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

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

The GDPR requires that individuals must be given certain key pieces of information about the use of their personal data by an organisation (the obligation on an organisation to give this information is known as transparency) and that this information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. This is stated to be particularly important where such information is being provided to children.

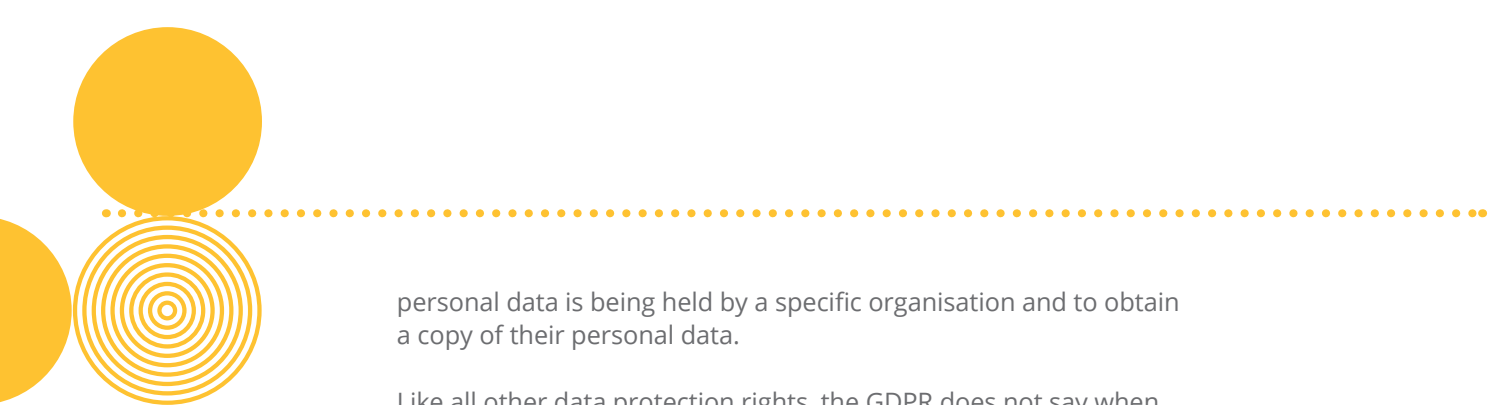
The transparency information that must be provided where an organisation is processing an individual's personal data includes the identity and contact details of the organisation who is collecting or using the personal data, the purposes and the justification (known as legal basis) for collecting or using the personal data, who the personal data is being shared with, how long it will be kept for, and what the individual's data protection rights are.

Questions:

1. What methods could organisations who collect and use children's personal data employ to easily convey this transparency information to children?
2. What approach should be used by organisations whose products or services are aimed at both adults and children? For example, should two separate sets of transparency information be provided that are each tailored according to the relevant audience?

(B) Right of access (Article 15 GDPR)

The right of access is one of the most important data protection rights because it allows individuals to find out whether their



personal data is being held by a specific organisation and to obtain a copy of their personal data.

Like all other data protection rights, the GDPR does not say when, or in what circumstances, a parent or guardian can make an access request for their child's personal data, or when or in what circumstances a child can make their own access request for their personal data.

Questions

3. At what age or in what circumstances should a child be able to make an access request to an organisation and receive a copy of their personal data? Is age the only relevant factor and if not, what other factors should be taken into consideration?
4. In what circumstances should a parent be able to make an access request and receive a copy of their child's personal data? Is there an upper age limit after which a parent should not be able to make an access request for their child's personal data? Are there circumstances where both the parent and child should have to jointly make an access request for the child's personal data?
5. How should the balance be struck between a parent's right to protect the best interests of their child and the child's right to privacy when organisations are dealing with access requests for the child's personal data?

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

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

Questions

6. At what age or in what circumstances should a child be able to make an erasure request to an organisation and have their personal data erased? Is age the only



relevant factor and if not, what other factors should be taken into consideration?

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

II. Safeguards

(A) Age verification (Article 8 GDPR)

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

Questions

8. If an online service provider is relying on consent as their legal basis (justification) for processing children's personal data, what methods could/should be used to verify that a child is 16 or over in order that the child is granted access to the online service without the need for parental consent?
9. (a) What methods could/should online service providers use to ensure that the person providing consent in these circumstances is *actually* the holder of parental responsibility over the child?

(b) What constitutes a "reasonable effort" made by organisations to verify such consent is being given by a person who is actually the holder of parental responsibility over the child? How should "reasonable efforts" be measured in this regard?
10. Prior to 25 May 2018, there was no law setting the age of digital consent in Ireland, but many online service providers required users to be at least 13. If an online service provider now is aware that an existing user of their



service is under 16, should the user be locked out of the service until they reach 16?

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

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

Questions

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

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

Profiling is a way of using someone's personal data to predict or analyse characteristics about that person, such as services they will be interested in, their likes or dislikes, preferences, views or opinions, or their behaviour, amongst other things. For example, organisations may collect information from their customers or users to try to predict other services or products they might be interested in.

A user profile can be a really valuable tool in revenue terms for an organisation because the detailed information on an individual contained in a profile can help the organisation to tailor information, advertisements and marketing materials, amongst other things, precisely to a person's interests, needs or individual views. For example, if an individual often clicks on posts online about a specific singer or "likes" pictures of clothes from a particular shop, they may start to see ads for tickets to that singer's concert or similar artists' concerts popping up on their social media feed, or ads might start appearing telling them that there is a sale on in that particular shop or similar shops. That is because online operators are constantly collecting and frequently sharing with each other this type of information about users and adding it to the profile being built about them. In this way, the user's profile then becomes the basis upon which specific advertising and marketing materials are selected to target that user.

The GDPR does not impose an outright prohibition on organisations marketing or advertising to children, but it does say that they should apply specific protections for children when marketing to them or creating user profiles. Additionally, collective guidance issued by the EU's data protection authorities (European Data Protection Board ("EDPB")) advises that, because children are



more vulnerable, organisations should, in general, refrain from creating individual profiles on children for marketing purposes. All individuals (including children) have the right to object at any time to their data being processed for direct marketing purposes.

Questions

12. In the case of marketing to a child, what factors should be taken into consideration when balancing an organisation's own legitimate interests in conducting direct marketing and the interests and rights of a child who is being marketed to?
13. Should organisations be prohibited from profiling children for marketing purposes? If so, should this be age-dependent or dependent on other factors? If so, what are these other factors?

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

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

Questions

14. What measures should organisations take to incorporate the principles of data protection by design and by default into the services and products that they offer to children?
15. Do you think products/services that are used by or offered to children should have built-in default privacy settings that vary according to the age and evolving capacities of a child? For example, should there be stricter privacy settings for younger children? How should these variations in the privacy settings be given effect?

V. General

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

