Joint Managerial Body

Submission

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

5th April 2019

Contact: [redacted]

I. CHILDREN AS DATA SUBJECTS AND THE EXERCISE OF THEIR DATA PROTECTION RIGHTS

Introduction

The Joint Managerial Body (JMB) was founded in 1964 to represent the interests of all voluntary secondary schools in the Republic of Ireland. It is the main decision-making and negotiating body for the management authorities of almost 380 voluntary secondary schools. The JMB comprises two founding organisations: AMCSS, the Association of Management of Catholic Secondary Schools and the ISA, the Irish School Heads' Association, representing the Protestant Schools in the State.

There are approximately 180,000 students in our schools ranging from age 12 to 18 years.

The responses below are provided from the organisational perspective of schools.

Context

In any matter relating to children, the child's best interests are of paramount importance.

Such an approach involves putting the interests and wellbeing of the child at the centre of all decisions and ensuring that the child's own voice is heard and respected as far as possible. For example, in the provision of health and social care to children, it is important that respect for their autonomy is integrated into decision-making in the same way as for adults.

This does not mean that the interests and views of parents or legal guardians will be displaced, as in most instances the child's interests will be best represented by its parents or legal guardians, although their interests are not the same.

Where children may not have the capacity to exercise their rights for themselves, they should nonetheless be as involved as possible in decision-making as even young children may have opinions regarding the use of their personal data.

Children with disabilities have the right to express their views freely on all matters affecting them, on an equal basis with other children, with their views being given due weight according to their age and maturity.

(A) TRANSPARENCY AND THE RIGHT TO BE INFORMED ABOUT USE OF PERSONAL DATA (ARTICLES 12-14 GDPR)

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

There is significant potential for organisations to use alternative modes of communication (e.g. audio, video, graphical modes) to supplement, or in some cases replace, the use of written notices. The publication by Data Protection Authorities of standardised icons (as promised under GDPR Article 12) could assist organisations in this regard. It has been well documented that many controllers, particularly organisations who regularly process children's data for purposes relating to social media etc., need to enhance their transparency offerings so that children have a better understanding of how their personal data is being used.

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?

It doesn't necessarily follow that organisations need to be presented with separate privacy notices. Clear and engaging privacy information, prepared with children in mind, will in many cases also be of great benefit to adults in development their understanding of processing activities.

(B) Right of access (Article 15 GDPR)

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?

It may not be appropriate that a specific age is identified for this purpose. All organisations who process children's data should understand that children as data subjects, regardless of age, have a right of access. How this right is to be best fulfilled will be influenced on context and circumstances. For example, when fulfilling an access request in an educational context, parents will often be the appropriate channel through which a controller will communicate.

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?

It may not be appropriate that a specific age is identified for this purpose. A controller who is processing an access request from a parent on behalf of a child, should have a level of confidence that the parent is acting in the best interest of the child. A controller will also need to remember that, where personal data is associated with the child as data subject, parental access to this data is granted to enable the best interests of the child to be protected. For nearly all access requests that are processed by schools, this is likely to be the case. In other circumstances (possibly as a result of some breakdown in family relationships for example) it may be that there is a clear divergence between the child's interests and the interests of a parent or parents. In these cases, the controller will need to take care that, in acting to fulfil an access request made by a parent, there is no interference with the child's rights.

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?

All family relationships, regardless of age, necessarily involve some sharing of personal data. The parent-child relationship is no different. Responsible parenting requires a level of involvement and oversight of a child's relationships, whether these are conducted in the physical or virtual worlds. Many parents conduct some monitoring of a child's electronic communications. At the same time, it needs to be understood that privacy is a fundamental right applicable to all data subjects, regardless of age. As children grow older they need to have the opportunity to develop and to take on the "ownership" of their own personal data, including the opportunity to make decisions in terms what personal data they choose to share and with whom. Again, parents recognise that that children must, with age, be given more autonomy and privacy in terms of the management of their own

information. Striking an appropriate balance is likely to require some form of risk assessment by the controller.

(C) Right to erasure

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?

The rights provided for under data protection legislation are open to all data subjects regardless of age. The legislation also recognises that children may be more exposed to risk as a consequence of their age. Organisations who are processing the personal data of children need to recognise their responsibilities in this regard. Some organisations may need to improve their "Right to Erasure" systems for example, particularly with regard to deleting data (images, videos etc.) where the child themselves has not been the source of the content. Other organisations may need to ensure that the act of erasure is not of itself problematic and does not interfere in some way with children accessing their rights in the future (e.g. possibly when they are adults).

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?

Circumstances may relate to social media accounts and exposure to online sexual content, material which promotes self-harm, nutritional deprivation, cyber-bullying – as examples.

The rights provided for under data protection legislation are open to all data subjects regardless of age.

In any matter relating to children, the child's best interests are of paramount importance.

Such an approach involves putting the interests and wellbeing of the child at the centre of all decisions and ensuring that the child's own voice is heard and respected as far as possible. For example, in the provision of health and social care to children, it is important that respect for their autonomy is integrated into decision-making in the same way as for adults.

This does not mean that the interests and views of parents or legal guardians will be displaced, as in most instances the child's interests will be best represented by its parents or legal guardians, although their interests are not the same.

Where children may not have the capacity to exercise their rights for themselves, they should nonetheless be as involved as possible in decision-making as even young children may have opinions regarding the use of their personal data.

Children with disabilities have the right to express their views freely on all matters affecting them, on an equal basis with other children, with their views being given due weight according to their age and maturity.

II. SAFEGUARDS

(A) AGE VERIFICATION (ARTICLE 8 GDPR)

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?

Social networking service providers need to ensure that maximum protection is provided for the accounts of minors. Therefore, the service providers should be required to respond as to how this verification might be further developed.

Examples:

A series of verification questions could be set up by which the parent or authorised parent wishing to access the service for their child is required to answer. The 'Terms of Use' should be linked to each of the verification questions and appear as pop-up boxes before a Yes/No or Accept button is clicked.

At its simplest, the person who authorised the consent would then be required to give their email and the service provider communicates a two-factor authentication process to them before there is access given to the 'child'.

Alternatively, the service provider does not give access until a required field under 'Terms of Use' is read and an explicit 'accept these terms' box is clicked upon.

Policy makers may be required to set down minimum verification requirements.

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?

A method may be where a clear message is set out at the point where the person is confirming consent on the service providers media platform.

The 'Terms of Use' are often ignored in the hastiness to join the social media platform or gain access to the information service providers platform. Make it more than one click to gain access or to accept the policy.

Examples:

A message should be posted up to create awareness around the fact that you are entering into a contract to accept these terms and conditions, you are signing in that you are the person with responsibility over the child and that where this information is false (through profiling/analytics of the account by the service provider) the account will be closed.

Policy makers perhaps should require service providers to take reasonable, proportionate and effective measures to ensure that the providers terms of use are enforced.

(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?

That the verification process is robust enough to demonstrate that the signing up process was clear, transparent and that two-factor authentication was in place.

Requiring the holder of parental responsibility to confirm and accept that they are giving permission and clearly understand the terms of use.

Again, policy makers perhaps should require service providers to take reasonable, proportionate and effective measures to ensure that the providers terms of use are enforced.

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?

Policy makers should require service providers to take reasonable, proportionate and effective measures to ensure that the providers terms of use are enforced.

When children are below 16, and parental consent is required, policy makers should require that reasonable efforts are made to verify that consent is given by the parent or legal representative of the child.

The question of user being locked out of the service should be addressed to the service providers.

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

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

Where Member States take measures to decide upon an age at which children are considered to be capable of consenting to the processing of personal data, their rights, views, best interests and evolving capacities must be taken into consideration.

Service providers should be required to monitor and evaluate usage while taking into account children's actual understanding of data collection practices and technological developments.

When children are of the compliance age of digital consent and parental consent is required, Member States should require that reasonable efforts are made to verify that consent is given by the parent or legal representative of the child.

III. PROFILING AND MARKETING ACTIVITIES CONCERNING CHILDREN (ARTICLES 21-22 GDPR)

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?

Recognising that personal data can be processed to the benefit of children, the data controller/organisations/service providers should take measures to ensure that children's personal data is processed fairly, lawfully, accurately and securely, for specific purposes and with the free, explicit, informed and unambiguous consent of the children and/or their parents or the person with parental responsibility.

The data minimisation principle should be respected, meaning that the personal data processing should be adequate, relevant and not excessive in relation to the purposes for which they are processed.

Data Subjects Rights clearly explained, for example:

Clear explicit consent and opt out options.

Privacy notices.

Right to know who your data is being shared with.

Right to erasure.

Right to complain.

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?

The above question infers that the answer will be that it is prohibited. This is a matter for policy makers.

The recommendation from the EU to Member States is that profiling for marketing purposes should be prohibited. The recommendation is: "With respect to direct marketing, the profiling of children, which is any form of automated processing of personal data which consists of applying a "profile" to a child, particularly in order to take decisions concerning the child or to analyse or predict his or her personal preferences, behaviour and attitudes, should be prohibited."

Factors:
The data controller/organisations/service providers should take measures to ensure that children's personal data is processed fairly, lawfully, accurately and securely, for specific purposes and with the free, explicit, informed and unambiguous consent of the children and/or their parents or the person with parental responsibility.

Require business enterprises and other relevant stakeholders to meet their responsibility to respect the rights of the child in the digital environment and encourage them to support and promote these rights.

IV. DATA PROTECTION BY DESIGN AND BY DEFAULT

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

Organisations should undertake due diligence in order to identify, prevent and mitigate their impact on the rights of the child in the digital environment. This would be referred to as a Data Protection Impact Assessment (DPIA).

A requirement perhaps that organisations perform regular child-rights risk assessments in relation to digital technologies, products, services and policies and to demonstrate that they are taking reasonable and proportionate measures to manage and mitigate such risks.

At a minimum encourage organisations to develop, apply and regularly review and evaluate child-oriented industry policies, standards and codes of conduct to maximise opportunities and address risks in the digital environment.

Recognising that parents, carers and others may rely on an online service's stated terms and conditions of service as a guide to the suitability of that service for their child, being mindful of available technologies and without prejudice to the liability of internet intermediaries, policy makers should require business enterprises to take reasonable, proportionate and effective measures to ensure that their terms and conditions of service are enforced.

Measures:

Evidence of a DPIA.

User testing.

Compliance audit.

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?

In all actions concerning children in the digital environment, the best interests of the child shall be a primary consideration.

The capacities of a child develop gradually from birth to the age of 18. Moreover, individual children reach different levels of maturity at different ages. Service providers should provide children with information on their rights, including their participation rights, in a way they can understand, and which is appropriate to their maturity and circumstances.

Policy makers and other relevant stakeholders should recognise the evolving capacities of children, including those of children with disabilities or in vulnerable situations, and ensure that policies and practices are adopted to respond to their respective needs in relation to the digital environment.

Awareness-raising in relation to online risks should be balanced and proportionate, and targeted at those most at risk of harm. There should be greater emphasis on digital safety skills to build resilience online.

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?

Adhering to best practice around safety by design and by default as per the Council of Europe's Recommendation adopted by the Council of Europe's Committee of Ministers 2018. Building on international and European legal instruments, the Recommendations provide comprehensive guidelines for action by European governments, including Ireland.

Recognising that children are entitled to receive support and guidance in their discovery and use of the digital environment, the policy makers should formulate legislation, policies and other measures to promote the realisation of the full array of the rights of the child in the digital environment and address the full range of ways in which the digital environment affects children's well-being and enjoyment of human rights.

Take into account the views and opinions of children.

[redacted]

5th April 2019

www.jmb.ie

Acknowledgement:
The JMB submission has been informed by the Council of Europe's Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment.
https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016808b79f7