TUSLA
An Ghníomhaireacht um Leanaí agus an Teaghlach
Child and Family Agency

DATA PROTECTION COMMISSION PUBLIC CONSULTATION: FUNDAMENTALS FOR A CHILD-ORIENTED APPROACH TO DATA PROCESSING

Observations by Tusla, Child and Family Agency

FINAL SUBMITTED v1.0 | 31.03.2021

Use of this Document

This document provides a response from Tusla, Child and Family Agency ("Tusla") to the Data Protection Commission in relation to the public consultation on the Fundamentals for a Child-Oriented Approach to Data Processing and is not intended for any other purposes.

This response has been written in the context of a child protection and welfare service and relates only to that context, specifically where relevant to the type of highly sensitive and complex personal data typically processed by Tusla.

This submission is being made by Tusla's Data Protection Officer (DPO) on behalf of and with input from the wider organisation, including the Executive GDPR Group.

Any questions in relation to this report can be directed in the first instance to Tusla's Data Protection Unit (DPU) by email to datacontroller@tusla.ie.

Introduction and Context

Tusla was established on January 1st, 2014 and is the dedicated State Agency responsible for improving wellbeing and outcomes for children in Ireland.

Tusla is a diverse and widespread organisation that operates across 17 geographical regions in Ireland, employs over 5,000 staff, and performs a vital role in the safeguarding of vulnerable children and families. In the performance of its role, Tusla handles high volumes of sensitive data and personal information. Tusla handles such personal data in both electronic and paper form, including names, addresses, medical details and information about confirmed or suspected cases of abuse toward children.

Tusla is an example of an organisation which, given the sensitivity and scale of personal data collected, stored and processed, must give consideration to the range of complexities and factors at play when it comes to balancing the requirements of data protection legislation and child protection legislation.

Tusla has a vested interest in ensuring that industry standards and best practice guidance give due consideration to the rights and welfare of the child as a data subject, whilst also recognising the complexities involved in protecting the personal data of children. Tusla's vision is an Ireland that is committed to the safety and well-being of children, young people and families. Every year, Tusla releases many publications and guidance on the welfare and rights of children in Ireland.

With that expertise in mind, Tusla previously made a submission to the Data Protection Commission (DPC) in 2019 on the first round of this public consultation, which is appended again for ease of reference. Tusla now welcomes the opportunity to provide a second response to this important consultation on the processing of children's data and is pleased to see that key points in our previous submission were taken into account by the DPC in drawing up the 'Fundamentals for a Child-Oriented Approach to Data Processing' ("the Fundamentals").

Tusla is happy to accept any additional queries or clarifications that the DPC may have in relation to this consultation response.

Tusla's Observations and Response to the Fundamentals

Observation 01: The Fundamentals for a Child-Oriented Approach to Data Processing (the "Fundamentals") aim to drive improvements in standards of data processing of children's data. The term "Fundamentals" has been used by the DPC to illustrate the critical nature of these standards and expectations.
Tusla's Response: Tusla welcomes the development of these "Fundamentals" and fully supports the DPC in their objective to improve standards and protections surrounding children's personal data. Tusla is also pleased to see that key considerations submitted by Tusla in part one of this consultation process (2019) have been incorporated into the Fundamentals and are embedded in the essence of these standards.

Observation 02: The Fundamentals will need to be complied with by all organisations that process children's data. This includes services that are directed at/intended for, or are likely to be accessed by children in both an online and offline world. The DPC also considers this to include "social services" contexts.
Tusla's Response: Based on the scope of applicability of these Fundamentals, and given that Tusla is an organisation that processes children's personal data, albeit in an 'offline' context, we will endeavour to adhere to these standards (where applicable) and embed them into all aspects of our work as the child and family protection agency.

Observation 03: Beyond this consultation, the DPC notes its intentions to consult with organisations under Section 32 obligations to draw up sectoral codes of conduct where children's personal data is processed, including social services providers.
Tusla's Response: Tusla would welcome the opportunity to work with the DPC in drawing up such sectoral codes of conduct and will await further instruction from the DPC on next steps for this engagement.

Observation 04: The final version of the "Fundamentals" will inform the DPC's approach to supervision, regulation and enforcement. Organisations will need to demonstrate that they are implementing the high levels of protection required under the GDPR for children's personal data which are aligned to these fundamentals.
Tusla's Response: Tusla is pleased to see that adherence to these Fundamentals will be monitored and enforced by the DPC. This will play a crucial role in protecting the welfare of children in Ireland, particularly with regard to the digital and online world. As the DPC will already be aware, given the nature of services delivered by Tusla and the subsequent sensitive nature of the personal data that Tusla processes, our Agency is already undergoing significant transformation efforts, driven by the GDPR Programme, to ensure that high levels of protection are implemented for all personal data processed by Tusla.

Observation 05: There are 14 x Fundamentals. The majority of these are aimed at online product/service providers which are not of relevance to Tusla. Some however, do have application and relevance in Tusla, particularly those relating to transparency and children as rights holders.

Tusla's Response: Whilst the majority of the Fundamentals appear to relate specifically to the digital world and to online service providers, Tusla will ensure that any relevancy of these Fundamentals within Tusla will be considered and implemented as a priority. Those of particular relevance to Tusla relate to transparency and the exercising of children's data protection rights. Tusla will consider these Fundamentals as a key priority under Phase 3 of the GDPR Programme.

Observation 06: The Fundamentals emphasise how children have the benefit of "specific protection" under the GDPR and as such, higher standards must apply when processing their personal data.

Tusla's Response: Again, Tusla welcome's the Fundamentals and is pleased to see that they call out the required "special protection" of children's personal data. This is a positive step towards driving higher standards of child specific data protection across all sectors and organisations in Ireland, which in turn will play a critical role to the welfare and general protection of those children. One of Tusla's key messages within the GDPR Programme that is being rolled out across the Agency is that we protect children and families by protecting their most sensitive personal data. Data protection must be embedded as a core part of everything we do on a day to day basis while delivering our critical services to children and families. It is assuring to see that this approach will be adopted and enforced across other sectors and organisations alike.

Observation 07: The Fundamentals are underpinned by the rights of the child (aligned to the UN Committee on the Rights of the Child) and the core message is that the best interests of the child must always be a primary consideration. The fundamentals in this context are applicable to any organisation where decisions are made in connection with the processing of children's data.

Tusla's Response: Tusla is pleased to see that the Fundamentals are underpinned in the rights and best interests of the child. This concept is at the heart of everything we do in Tusla. It is aligned with our core statutory remit, our practice delivery model, and of course is in keeping with the Children First Act 2015. This alignment emphasises to all organisations, including Tusla, that data protection plays a crucial role in child protection and that these Fundamentals should be a part of, not apart from, all service delivery models that process children's data.

Observation 08: "The DPC's position is that child protection/welfare measures should always take precedence over data protection considerations affecting an individual. The GDPR, and data protection in general, should not be used as an excuse, blocker or obstacle to sharing information where doing so is necessary to protect the vital interests of a child or children."

Tusla's Response: Tusla notes and welcomes the DPC's position with regard to the balance of data protection legislation and child protection and welfare. It is reassuring to know that the DPC holds the same view as Tusla on this matter, that is, data protection rules should never be a barrier to safeguarding or protecting children (and adults alike) from violence, abuse, interference or control by any party. This is an Agency-wide position adopted in Tusla (supported by Tusla's Data Protection Officer and Senior Leadership Team) and one which we are continuously communicating to our front-line staff who deliver critical services to children and families on a daily basis. We adopt this approach in our day-to-day practice as well as in our engagement with other critical state bodies (e.g. An Garda Síochána when investigating matters of offences against children). Our dedicated GDPR Programme ultimately aims to drive this message throughput our Agency by supporting improvements in Tusla's data protection and control environment whilst balancing the complexities surrounding child protection and welfare.

Observation 09: When a child wishes to exercise their data protection rights, a range of factors must be considered by the data controller. As set out in the Fundamentals, this includes the age and maturity of the child; the type of request; the nature and context for processing and type of service provided; the type of personal data; the best interests of the child; and if the child is exercising their rights with assistance from an adult/third party. Where an organisation decides not to facilitate a child in exercising their data protection rights, they need to explain the rationale to the child in a transparent way.

Tusla's Response: Tusla is pleased to see that the DPC has considered some of the key points made in its previous submission to this consultation. Age alone is not enough of a measure and must be considered alongside some other important complicating factors when facilitating a child to exercise their rights.

In the specific context of Tusla's services it is important, for example, to understand whether or not the child has the maturity level or the capacity to cope with the information provided, particularly if it relates to highly sensitive content such as details of neglect or abuse. As outlined in observation 08, *data* protection should never take precedence over *child* protection and it is important for a data controller to always consider whether or not the child will be at risk of harm when exercising these rights.

Where organisations do facilitate a child in exercising their right, it is of crucial importance that supports are put in place for a child to understand the information that is provided, particularly where the personal data is highly sensitive (e.g. support could be provided by professionals who engage with the child to help them understand and deal with the information/content of the sensitive data).

As set out in our 2019 submission, Tusla endorses the DPC's approach to the removal of all barriers or unnecessary obstacles for children in exercising their rights. Tusla is of the view that data controllers must give paramountcy to the best interest of the child in all activities relating to the processing of children's data. Putting the best interest of the child at the heart of any approach to facilitating data subject rights will always require a data controller to undertake a risk assessment of the nature, context and processing of that child's data in order to ensure that appropriate safeguards are implemented to protect that child not only during the course of the processing of his or her data but also during the facilitation of his or her exercise of his or her data protection or other fundamental rights.

Given the unique context of Tusla's processing, Tusla is also mindful of how disclosure of personal data relating to social work and medical and health records is moderated through relevant professionals, pursuant to relevant statutory instruments where it is appropriate to do so, to prevent the data subject from any harm that a direct disclosure (through response to any access request) may otherwise cause. Tusla suggests that it is appropriate for data controllers to take into account the best interest of the child when responding to an access request in relation to a child's personal data and consider whether disclosure is best moderated through an appropriate adult in some circumstances rather than the child him or herself. Similarly, the exercising of rights relating to erasure or rectification also brings to fore a series of complexities (e.g. retention periods particularly in a child protection and social services context) and so too must be given due consideration by data controllers or relevant professionals where appropriate as part of the decision making process.

Tusla is of the view that all data controllers should seek, as far as possible, to facilitate a child's data protection rights and considers that a lawful limitation or restriction on these rights is not per se a refusal to facilitate such rights, rather it is an acknowledgement that data protection rights are not absolute and it is often the case that these rights must be carefully balanced with other fundamental rights in order to preserve a democratic society.

However, Tusla does endorse the spirit of the Fundamentals in this regard and consider that it is incumbent, indeed it is a legal requirement, on all data controllers who seek to lawfully limit or restrict any data protection rights, including those of a child, to explain in full any limitations or restrictions relied upon in the curtailing of these rights in any particular circumstance. Tusla further considers that is incumbent on any data controller seeking to curtail a child's data protection rights to review that period of curtailment and lift any limitations or restrictions once they no longer lawfully apply and to advise the child or his or her appropriate adult of any such change in circumstance so that an opportunity can be afforded to the child at the relevant time to exercise his or her data protection rights.

Observation 10: Parents/legal guardians may exercise their child's rights if it is in the child's best interest to do so. When a parent/guardian is exercising their child's rights, the data controller should consider a range of factors, including the age of the child; the nature and sensitivity of the personal data; the nature of the relationship with the child; the purpose for exercising the rights; any views/opinions expressed by the child; the risk of harm/distress to the child; and/or any sectoral rules or laws that may apply.

Tusla's Response: In its submission of 2019, Tusla outlined a number of factors that should be considered when a parent or legal guardian is exercising data protection rights on behalf of the child. In its submission, Tusla gave specific examples of complex scenarios which give rise to the need for such considerations. Tusla is pleased to see that the DPC has considered such factors and has embedded these into the Fundamentals. The nature of the relationship between the child and parent/legal guardian for example is of crucial importance, particularly in the context of social services settings. A number of factors may be at play when a parent exercises a child's rights on their behalf, and it is of critical importance that these factors be considered e.g. it cannot be assumed that a parent is always the legal guardian of the child, likewise it cannot always be assumed that a parent intends to use the information in the child's best interests. Again, to reiterate observation 08, data protection should never take precedence over child protection and it is important for a data controller to always consider the broader context when a parent is exercising a child's rights. In the context of the services that Tusla provides, this must always include the child protection dimension.

Observation 11: Transparency is a freestanding right for children and the Fundamentals (particularly Fundamentals 5 and 6) place an onus on organisations to ensure meaningful transparency for children when processing their data.

Tusla's Response: The position of Tusla held in its previous submission of 2019 is aligned to those captured in these Fundamentals, that is, a child should be informed about how a data controller processes his or her data in a meaningful and accessible way that is clear and easily understood by the child. Tusla is of the view that all data controllers who engage with children should communicate with them in a clear and meaningful way, and those who process children's personal data in particular should tailor their notices and transparency information to be accessible to children of all ages and capacities. Tusla gave an example of its new website changingfutures.ie which was developed by children for children who use Tusla services. The website contains tailored information and language appropriate to different age groups, and conveys key messages in a range of ways including cartoons, videos and graphical imagery. For example, the image below is from the 6-9-year-old section of the changingfutures.ie website. This explains what Tusla does in an animated video rather than in text to be meaningful for the children using the website. Similar approaches could be adopted by organisations to convey transparency messages in adherence with these new Fundamentals. In response to these Fundamentals, Tusla will endeavour to review its

transparency information provided to children and ensure that it meets the requirements of being clear and meaningful to children.

What is Tusla?

Tusla help make sure children and young people are safe and looked after. Play this video to learn more.

Observation 12: The GDPR identifies children as vulnerable natural persons needing "specific protection". The EDPB guidelines further lists 'vulnerable data subjects' as one of the criteria that could trigger the need for a DPIA. The DPC will consider this a key part of compliance in organisations that process children's data: "A child-oriented 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 with existing legal requirements for protecting the position of children as data subjects"

Tusla's Response: Tusla notes the DPC's position with regard to child-oriented DPIAs and is pleased to see that this will be considered a key part of compliance for all organisations and sectors. As per the points made above in observations 1 - 11, Tusla believes that effective data protection contributes to effective child protection and as such welcomes this approach by the DPC.

Tusla has also recently revised its DPIA Policy and at the heart of this policy is the need to embed data protection by design and default, particularly given the sensitivity and nature of the data processed by Tusla and the relevancy of our services with regard to children. As Tusla has a statutory duty under section 8 of the Child and Family Agency Act 2013 to have regard to the best interests of the child when making decisions in relation to the performance of its functions and to regard the best interest of the child as the paramount consideration when performing its function in relation to the individual child. Tusla's DPIA Policy expressly states, in relation to high risk processing criteria that trigger the requirement for a mandatory DPIA "[*T*]*he personal data processed by Tusla by its nature relates to individuals who are often extremely vulnerable (this is indicated by the nature of the services provided to and accessed by Service Users) and in many instances to children".* Tusla is of the view that this new DPIA Policy is aligned to these Fundamentals and that it can demonstrate compliance with a child-oriented approach to DPIAs as, notwithstanding our criteria for assessment of risk including necessarily that Tusla processes children's personal data and that therefore special protections must be afforded to both that data and the data subject to whom that data relates, a child-oriented approach to data protection risk assessment is entirely compatible with Tusla's statutory duty to give primacy to the best interests of the child in the discharge of its functions. However, Tusla would welcome further specific guidance from the DPC on what specifically constitutes a 'child-oriented DPIA' so as to ensure we can meet those requirements.

Conclusion

Tusla supports and welcomes the development of these Fundamentals and is pleased to see that they take into consideration the complexities of the GDPR in the context of child protection and welfare services. The best interests of the child have always been paramount to Tusla's organisational and strategic vision and it is reassuring to see that the Fundamentals align with this vison.

Our position as the child and family protection agency has always been that data protection should never take precedence over, nor be a blocker to, child and family protection. That being said, the DPC will already be aware of Tusla's GDPR Programme, which has now successfully moved into Phase 3 with significant investment, support and commitment from all levels of staff within Tusla. This programme aims to drive to improvements in compliance and embed data protection into everything we do in Tusla. As such, Tusla will commit to considering the final version of the Fundamentals once published and will include them as a core part of our work programme over the next three years as we continue to implement and embed the required changes for our data protection and control environment.

Tusla is happy to accept any clarification questions that the DPC may have in relation to this response.

APPENDIX

Tusla's Submission of 2019

(part one of DPC's Public Consultation)

DPC Public Consultation of 19th December 2018

The processing of children's personal data and the rights of children as data subjects under the General Data Protection Regulation.

Tusla Management Response | 5th April 2019

Final v1.0

TUSLA An Ghníomhaireacht um Leanaí agus an Teaghlach Child and Family Agency

Table of Contents

Use of this Report

This report provides a response from Tusla, to the Data Protection Commission (DPC), in relation to the public consultation on the processing of children's personal data and the rights of children as data subjects under the General Data Protection Regulation (GDPR). This document was written in the context of a child protection and welfare service, and relates specifically in parts to the type of highly sensitive and complex personal information typically held by the Tusla.

This response was compiled by Tusla's Data Protection Unit (DPU) with input received from the wider organisation and Senior Management Team (SMT).

Any questions in relation to this report can be directed to Tusla's Data Protection Officer (DPO) by email to datacontroller@tusla.ie in the first instance.

Introduction and Context

Tusla was established on January 1st, 2014, by the amalgamation the Health Service Executive (HSE) Children and Family Services, the Family Support Agency, the National Educational Welfare Board, and a range of services focused on responding to domestic, sexual, and gender-based violence. Tusla is now the dedicated State Agency responsible for improving wellbeing and outcomes for children in Ireland.

The Agency is a diverse and widespread organisation that operates across 17 geographical regions in Ireland, employs over 4,000 staff, and performs a vital role in the safeguarding of vulnerable children and families. In the performance of its role, Tusla handles high volumes of sensitive data and personal information. Tusla handles such personal data in both electronic and paper form, including names, addresses, medical details and information about confirmed/suspected cases of abuse toward children. Tusla is an example of an organisation which, given the sensitivity and scale of personal data collected, stored and processed, must give consideration to the range of complexities and factors at play when it comes to children exercising their rights under the GDPR.

Tusla's vision is an Ireland that is committed to the safety and well-being of children, young people and families. Every year, Tusla releases many publications and guidance on the welfare and rights of children in Ireland. With that expertise in mind, Tusla welcomes the opportunity to provide a response to this important public consultation on the processing of children's data and the rights of children as data subjects under the GDPR.

It is our hope that the responses provided herein will contribute to the drawing up of effective, well-reasoned guidance materials and codes of conduct in relation to the processing of children's data, that recognise the complexities involved in protecting the personal data of children. Tusla's priority is to ensure that industry standards and best practices give due consideration to the rights and welfare of the child as a data subject. From that perspective, we are happy to accept any additional queries or clarifications that may be required by the DPC following a review of this response.

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)

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

Tusla's position is that there are numerous methods and tools organisations can utilise to ensure that information about the processing of personal data is conveyed easily and in an understandable manner to children. A selection of these methods are outlined below.

Child-friendly information materials

- It is recommended that organisations develop a service for young people to provide information on how and why their data is processed using child-friendly materials such an **information leaflets, visual infographics, or video mediums such as cartoons**. It is recommended that these materials appeal to younger audiences and grasp their attention to convey messages about data processing in a way that they will understand.

Visual privacy notices

- Organisations could develop **simple, visual versions of privacy notices and policies** to inform children about how and why their data is processed. These items would preferably be infographic style visuals which use plain language (with no ambiguity) to help children understand the key messages being communicated.

Accessibility of information

- Accessibility of information is a key factor for consideration when conveying transparency information to children. For example, not all children have access to online information and services, therefore practical methods of providing the information to children should be considered, such as the **provision and display of hardcopy leaflets/posters.**

- The provision of clear messaging and plain language (in a variety of languages) is also an important consideration when it comes to providing information to children. Organisations should avoid overloading children with information, and instead provide it in a concise, simplistic manner. The age of the child also plays a part in this. For example, best practice research methods suggest children under the age of seven should be provided with information in **graphics and plain language**, whereas children over the age of eight should be given information with slightly more text, and young persons between the ages of 16-18 should be provided with information at a similar level to those of adults. In Tusla, social workers use TACTIC packs (meaning 'Teenagers and Children Talking in Care'). These packs are tailored for different age groups to ensure accessibility for children. The images below are extracts taken from the TACTIC 'Me and My Care Plan' review form. These forms are used nationally by social workers who engage with children of all ages.

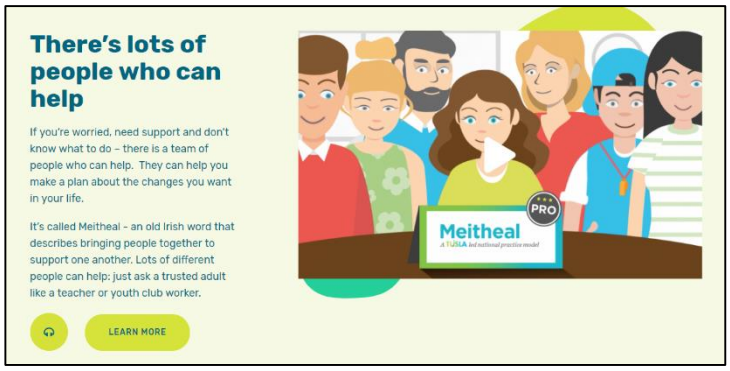
5 to 8 years old

8 to 12 years old

13 to 18 years old

- Media for communicating transparency could also be considered in the context of communication channels. **Child-friendly websites, face to face communication, communication in writing, and social media** all have varying degrees of effectiveness when it comes to communicating key messages with children and should be considered when providing data privacy transparency information to children.

- The **child's capacity to understand** key messaging and assimilate the information should also be considered. Young people should be given time to ask questions and to digest the information that is being provided. Consideration should also be given to young people with **literacy and / or intellectual capacity** issues. For example, Tusla recently launched a new child friendly website www.changingfutures.ie which is tailored to varying age groups and intellectual capabilities by providing information through different methods, such as written text, audio notes and video, as shown in the screen clip below. The idea for the website was developed by young adults with lived experience of Tusla as part of a Youth Participation Project. Young people were involved in every stage of the development of the website to ensure the website communicated information appropriately for young people.



- In addition to the child's capacity to understand and digest information provided, a key consideration regarding young people, particularly those in care or who may have experienced adverse events/trauma and may be suspicious of state agencies, is **how to convey difficult, technical information** in a suitable way within the boundaries of professional relationships.

- Organisations may also want to consider, where appropriate, the need to provide additional **training to staff on how to deliver transparency information** to children, particularly in cases where staff engage with children and young people directly.

- Finally, it is recommended that methods of communicating to children, and the materials being used, be tested to **ensure they are fit for purpose**. This should include focus groups with children to pilot and assess whether the materials provided are clear and easily understood. Communicating important messages to children is also not just a once off event. It is important that the information be revisited one-to-one with children, either through written, visual or verbal means as appropriate.

In the context of the DPC, Tusla would suggest that as part of its proposed guidance materials, the regulatory body could provide organisations with tried and tested sample templates (e.g. child-friendly privacy notices and information leaflets), which organisations could then tailor to align with their specific policies and processes.

Question 2 | "What approach should be used by organisations whose products or services are aimed at both adults and children? For example, should two separates sets of transparency information be provided that are each tailored according to the relevant audience?

Where young children and adults are both engaged by the same organisation, it is Tusla's recommendation that transparency information **should be tailored** to suit the differing audiences and service users that exist, depending on their age profile and capacity. For example, a privacy policy could exist in the form of a visual poster/animation for children under the age of seven and in the form of a more detailed policy document for adults over the age of 18. In both cases, plain language should be used and clear messaging applied. Where common ground can be found to create a one-size-fits-all model, this may be an appropriate approach. For example, it might be possible to preface a detailed information leaflet with a plain language/pictorial summary for children in cases where an organisation does not wish to create an explicit separation of information for children and adults.

The key factor for consideration here is that organisations should convey the **same message**, but in different formats. No variances should exist between the two regarding the core meaning of the message being communicated.

***Note**:* As an example, in line with the organisation's commitment to child protection and information transparency, Tusla will be preparing a child friendly version of its privacy policies as part of 2019-2020 activity.

(B) Right of access (Article 15 GDPR)

Question 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?"

While Tusla does not suggest creating any unnecessary obstacles for a child in accessing their data, there are a number of important, **complicating factors, alongside age, that must be taken into consideration** by organisations before access is granted, and cases where exemptions to this right should exist. These include:

- The degree to which the parent or guardian is involved in, or known to, the service provider;
- The **nature of the information** and level of sensitive data included in the content;
- The **risk of the information causing additional, and perhaps unintended, harm or trauma** to the child e.g. information about adoption or family abuse;
- The **maturity level of the child and their capacity** to cope with the information provided (an assessment should be made by professionals who engage with the child to decide if they can cope emotionally with the content); and
- The **behavioural history** of the child (e.g. history of self-harm, violence etc.).

When access to sensitive information is granted to a child, support should be provided by professionals who engage with the child to help them understand and deal with the information/content of data. For example, in Tusla, the narrative created by a case file may be alienating to a child, and it is therefore important for our social workers to support them to understand the information and appropriately manage any exposure to the contents of a file in the context of their wider personal circumstances.

Question 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?"

As noted in the response to Question 3, there should be no unnecessary obstacles in place for a child or parent in accessing personal data, however there are a number of **important factors that should be taken into consideration** by organisations before access is granted, and cases where exemptions to granting parents access to their child's information exist. These include:

- The **legal relationship** between the parent and the child i.e. whether or not the parent is the legal guardian;
- The **capacity of the child**, i.e. the parent may have the ability to access the child's personal data in cases where the child does not have the capacity to do so;
- The **expectation of confidentiality of the child,** i.e. if the child is of an appropriate capacity and wishes to deny the parent access to their information and to keep personal details confidential, the underlying reasons for this must be considered;
- The **capacity and health of the parent**, including the stability and soundness to use the information in the best interests of the child;
- The **past and present behaviours of the parent**, including relevant criminal history, substance abuse and any adverse behaviour that has been/is being directed toward the child; and
- The **intentions of the parent,** including whether the parent is acting as an advocate of the child and their intent to use the information in the child's best interest.

If a parent requests access to a child's personal information, and the child wishes to withhold access, organisations may consider upholding the right of the child and denying the parent access if it is deemed that the child possesses an appropriate level of capacity and maturity. If a child wishes for the access to be granted, a process could be in place to support a joint request to be made.

Note: Consideration should still be given as to whether or not the child is providing their consent voluntarily or under duress by the parent.

A process for joint requests may also be appropriate in cases where the child possesses the appropriate capacity, but the information is likely to cause them harm or distress, and therefore requires appropriate parental support. There may be situations, however, where parental consent should not be a barrier to a child who is otherwise appropriately supported e.g. in alternative care and wishes to access their data under the supervision of an appropriate alternative guardian.

In addition, there may be circumstances where requiring guardian consent for a child to access a service would put them at risk of harm. Under these circumstances, and in line with Recital 38 of the GDPR, it is Tusla's recommendation that the child should be able to consent for themselves even if they are under the legal age.

The table below outlines some scenarios which highlight some of the complexities for consideration in relation to Question 4.

Scenario 4.1:

Complicating Factor: Strong negative sentiment felt towards the parent by the child.

Scenario Description:

- A parent may request their child's information but the child may have strong negative feelings towards the parent;
- There is no related conviction against the parent and they hold full guardianship rights over the child.

This may be a circumstance where both the parent and child should have to jointly make an access request for the child's personal data.

Scenario 4.2:

Complicating Factor: The parent of a child who is on the Child Protection Notification System (CPNS) or is the subject of a court order, seeks information about the child and/or family.

Scenario Description:

- Information is gathered about a child as part of their engagement with Tusla;
- A parent requests their child's data but that parent has been convicted of abuse against the child.

This may be a circumstance where the parent is denied access to information on the grounds of S.I. No. 83/1989 – Data Protection (Access Modification) (Social Work) Regulations, 1989. In accordance with this statutory instrument, "information constituting social work data shall not be supplied by or on behalf of a data controller to the data subject concerned in response to a request under Section 4(1) (a) of the Act if it would be likely to cause serious harm to the physical or mental health of the data subject".

This exemption relates to the data subject (i.e. the child) and not the parent. Here, the parent, who is not the data subject, is seeking information held about the child, which we might consider withholding if we believe it would cause harm to the child.

Scenario 4.3:

Complicating Factor: The child, who is of an appropriate age and capacity, has an expectation that personal information will be kept confidential.

Scenario Description:

- A child is openly engaging with a social worker with the expectation that the conversation is confidential and that details will not be released to the parent;
- A parent subsequently requests the child's information.

This may be a circumstance where the consent of both the parent and child is required in order to process an access request for the child's personal data.

Note: the outcome of each case will be dependent on its unique circumstances.

In conclusion, it would be beneficial for the DPC to develop specific evidence informed guidelines taking into account the potential risks and benefits to an individual in accessing and assimilating information about themselves. Such guidance could direct service providers in assessing and providing for support needs associated with the release of information.

Question 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?"

The Health Information and Quality Authority (HIQA) National Standards for the Protection and Welfare of Children state that children and families should have access to personal information held by the service in compliance with legislation and in the best interests of the child. In this context, it should not be taken for granted that a parent or guardian is always acting in these best interests. As per the Children First Act 2015, and in keeping with HIQA's National Standards, it is crucially important that organisations consider this and have a process in place to ascertain the best interests of the child first when dealing with parental requests for access to their child's data.

Tusla believes that a risk and benefit assessment of releasing the child's information should be the primary decision driver when it comes to balancing the interests of the parent and protecting the child's privacy. This should be carried out by professionals or advocates who engage with the child and understand the context of their situation. For example, if a parent does not want information released in order to protect the child from harm or emotional trauma, then it may be appropriate to favour in the case of the parent, subject to assessment by an independent professional or social worker. However, if no harm will come to the child by releasing the information (or if harm is possible but the child is deemed to have the capacity and/or alternative supports in place to cope with the information), but the parent does not want the files released in their own interest, then it may be appropriate to act in favour of the child's request and grant them access to their personal information.

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

Question 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?"

As highlighted by Dr. Geoffrey Shannon, Special Rapporteur on Child Protection, in his address to the Oireachtas on cyber security for children, the child's right to be forgotten should be provided for in all possible circumstances. As per the response to Question 2, the **age of a child is not the only relevant factor** when it comes to their ability to exercise their rights under the GDPR. Instead, their comprehension, their cognitive/emotional maturity, and what the information may be used for now, and in the future, should be considered. A number of other important factors also need to be assessed, particularly in relation to erasure requests. These include:

- The type of personal data/information held and the **complex nature of some case files/reports**. For example, family case reports may contain information on more than one child and an erasure of the data may only be possible if all siblings mentioned in the file agree to that request;
- The justification or **legal basis** for retaining the data, i.e. court files or case reports which may be required for future cases. For example, there are situations where allegations are made years after a child has used a service (retrospective allegations), and the only evidence as to what was happening at that time, in for example a residential unit, is the case records;
- The future implications and **impact to the child** should the information be deleted. For example, whether the information may benefit the child in the future or negatively impact them in the long term if it is erased;
- The child's **capacity to understand** the information being erased and the impact/consequences of erasing the data requested;
- The **reason** for the request. For example, there may be situations where a state agency's record of an event does not align with a family's account of the event which may result in an erasure request (particularly if that account bears authority in being a record from a state service). In this case, a fair process for **review and amendment** of information, rather than erasure, should be considered;
- Whether the child seeks to **withdraw initial consent** provided to process information, and subsequently seeks to have personal information about them deleted; and
- Whether the child is acting of their **own free will** and in their own interest and not requesting erasure under duress to the benefit of another individual.

It is important that an assessment be undertaken for each erasure request regarding children's personal information and that organisations ensure appropriate policies, and associated training, on record keeping are provided to support good practice and ensure the rights, and best interests, of the child are upheld.

Question 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?"

As per the response to Question 6, it can be potentially harmful to erase a record of something that an individual may need to recall or revisit later in life, and there are circumstances where it may not be appropriate for a parent to request erasure of their child's personal data. This primarily depends on the type of service provided and the nature of the personal data requested for erasure. Echoing the

responses above, an assessment in these cases should be carried out to make sure the request is not submitted in the interest of a parent rather than the child concerned.

That being said, it could be also be stated that there are cases where a parent should be granted the right to request erasure of the child's personal data, with due regard to the best interests of the child. These factors for consideration include;

- If a child has put themselves in **danger or is at risk of exposure** of their personal data and the parent is protecting their best interests e.g. if a child uploads an inappropriate photo of themselves to a website;
- If a child does not have the **capacity** to understand the implications of their data being held by an organisation; and
- If a child **unknowingly or involuntarily provided consent** for their information to be held e.g. through direct marketing or online gaming advertisements.

In particular, it is a generally accepted principle of data protection that in scenarios where a child is not competent to provide consent due to not having the capacity to understand the implications, it is often in the best interests of the child for the parent / guardian to act on their behalf. Tusla's position is that it may be beneficial for this principle to also apply in the three additional scenarios presented above, particularly in instances where the child has not yet reached the digital age of consent.

II. Safeguards

(A) Age verification (Article 8 GDPR)

Question 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?"

Online verification of age is an issue which has yet to be addressed by many organisations across many countries, and is a gap in the online industry which unfortunately places children at high risk of exposure to inappropriate services, advertising and virtual networks that could potentially cause harm.

At present, Tusla does not provide any online services which specifically target children (aside from providing information about relevant services). This may change, however, as part of the Agency's wider transformation strategy. Tusla's standard approach does however, request verification of ID in relation to data subject access requests, and similar measures of verification could be applied for online services.

It is recommended that organisations ensure that appropriate processes are in place to delete, and verify the deletion of validated and rejected IDs when they are no longer required for the purpose for which they were originally processed. It is further recommended that privacy impact assessments conducted on any new technologies consider the impact on children where they are likely to be a key service user.

Question 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?"

If a parent or legal guardian is providing consent on behalf of a child, it may be appropriate for organisations to request some form of valid identification from the person providing consent in an attempt to demonstrate parental responsibility or guardianship. The use of this method would have to be proportionate in the circumstances and dependent on the type of service being provided. Organisations should consider deletion or destruction policies in relation to this type of validating identification to ensure that it is not kept or processed for any other purpose.

Question 9(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?"

Reasonable effort could be defined as an organisation that requests verification of ID (as outlined above) and grants or denies access based on an appropriate review and assessment of the documentation provided. In a Tusla-specific context, the Agency's Data Protection Unit requests third party verification of ID as part of core processing activities such as subject access requests. Where information is not provided or deemed invalid, access is denied to protect the best interests of the child.

Note: this will be dependent on the nature of the organisation and the services it provides.

Question 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?"

As the digital age of consent in Ireland (under the Data Protection Act 2018) is 16, it is Tusla's view, as per the response to Question 8, that all existing users of a service should be required to verify their age. It may be appropriate for any users under the age of 16 to be blocked from continuing use of the service unless valid parental consent is provided on their behalf.

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

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

While Tusla's organisational competencies are not technology-based, the following are suggestions which could facilitate compliance with the various ages of digital consent in different Member States:

- Check the location of the user so that the age of consent is automatically updated depending on the jurisdiction within which the service user is based
- Have multiple website domains that are tailored based on the laws within the jurisdiction of the service user

Note: the points above assume the determining factor to confirm what digital age of consent applies is where the child is based, and that they are not using a personal virtual private network (VPN) service to disguise their location.

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

Question 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?"

Marketing to children is not prevented under GDPR, but it is Tusla's view that, when marketing to children, all necessary steps should be taken to ensure no aspects of child protection and welfare, or GDPR, are infringed.

For protection purposes, **no *direct* marketing should target a specific child**. This is largely due to the child's reduced ability to understand the purpose underpinning the marketing as well as the implications/potential risks of providing any personal data (including those of others) in response.

When marketing in a generic/indirect manner to children, the following should be considered:

- **The impact of the content on the child** – including whether the content would cause any physical, mental or moral harm to children exposed to it;
- **Transparency –** including clear statements to ensure that children understand the purposes underpinning the marketing;
- **Language –** the language used should be clear and should in no way take advantage of the child's level of understanding/cognitive ability or in any way exploit the vulnerabilities of a child; and
- **The channel used for the communication –** including ensuring that the marketing channels used are appropriate for the age category of the child.

Question 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?"

Recital 71 of the GDPR states that profiling should not apply to children, but the Article 29 Working Party clarifies that this is not an absolute restriction, and profiling may sometimes be necessary to protect their welfare. Tusla's position is that, in line with this interpretation, profiling should never apply to children for commercial marketing purposes and should be subject to a legal basis, such as public interest. Profiling activity should be age-dependent and should not occur until the child is legally allowed to give consent under GDPR.

Where profiling occurs on children who are old enough to provide consent under GDPR but are under 18, at a very minimum, Tusla believes that strong safeguards should be put in place. Clear information should be provided on how the child's personal data is being processed for the explicit purpose of profiling. The ability to object to profiling should be easily accessible and understandable for children. If they object, processing should stop immediately. Data Controllers must be able to demonstrate the safeguards that are in place to protect children.

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

Question 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?"

From Tusla's perspective, it is suggested that organisations offering services/products to children incorporate the following aspects into the design of such services/products to ensure data protection principles are embedded throughout:

- All processes should be designed with children in mind regardless of whether they are the sole age category or not;
- During the planning stages of any service or product, whether it be new or a re-design of an existing product/service, a Data Protection Impact Assessment (DPIA) should be conducted. The risk to children that this new/improved service or product may pose should be assessed. If it is believed there is a risk and there are appropriate safeguards in place to protect children the project may go ahead. If there is a risk with no mitigation available, the project should not be undertaken;
- Where possible, ensure that the legal basis for processing is not solely consent. This ensures the processing activity is required and protects children from unnecessary processing;
- Where consent is the sole legal basis for processing ensure it is communicated to the child in clear and understandable language. The child should fully comprehend the implications of the processing they are giving consent to;
- Where a guardian is providing consent on behalf of a child, ensure mechanisms are in place to verify the legitimacy of the guardian (as also mentioned in Question 9a);
- Where guardian consent is required for a child to access services, and obtaining that consent may put the child in danger, the child should be able to consent for themselves even if they are under the legal age;
- When a child's age needs to be verified online, ensure there are robust safeguards to verify the age of a child;
- Where consent has been used as a legal basis, ensure strong processes for erasure are in place for individuals who gave consent when they were children;
- As the age of child consent varies across the jurisdictions in the EU, ensure processes that require the consent of a child are tailored across all countries to meet the requirements of that location;
- Privacy notices should be written in plain language that can be understood by a child, and across multiple languages
- All information that is relating to privacy should be displayed in a child friendly format that will allow them to understand the information;
- Processes for executing data subject rights should be simple so a child of any age can avail of them and they should be easily located to ensure a child can avail of their rights;
- All companies that provide services or products to children should have child safeguard statements clearly defined in a publicly available format;
- Each company that provides services or products to children should have a designated person for child protection. This person will represent the child in different matters to ensure their rights are protected at all stages of business processes;
- Adequate training should be provided to all employees that handle or are in contact with children's personal data. This should go as far to include training on how to effectively carry out services while implementing practices to protect their data. Training should be provided on note taking to ensure information is recorded only if necessary and the information is protected throughout its lifecycle;

- Procedures should be created for each process that handles a child's personal data or has direct interaction with a child. These procedures should detail how to adequately protect the child's data at each stage of the process;
- Guidance should be provided on record-keeping and information sharing. There should be clear guidelines on what notes can be taken, in what format and for how long the notes should be retained e.g. hand written paper notes should be transcribed into electronic format as soon as possible and the paper version should be shredded; and
- A disciplinary procedure should be in place for employees that have been provided with sufficient training and guidance and do not follow company policy and put a child at risk due to misuse of their information.

Question 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?"

All products and services offered to children should have built-in privacy settings. This is important as children learn through trial and error without always realising the potential consequences of their actions. This could lead to them providing personal information without thinking about the consequences of it first. It may however be hard to make privacy settings age specific for evolving capacities/maturity levels as children evolve at different rates. This could lead to some children being negatively impacted if privacy safeguards are reduced for their age group.

The change of privacy settings may occur at the age of consent for GDPR and at 18 when children transition to be treated as an adult. Products/services should ensure that privacy settings are easily accessible and understandable for children of all ages and stages of maturity. The right to be forgotten should be easily accessible and understandable for children and for their legal guardians where appropriate. Where parental consent is required, controls should be in place to enable the parent to verify their legal guardianship. Services should ensure that there is no profiling or direct marketing conducted to children, however if this practice must take place, it should be restricted and age dependent.

V. General

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

With regard to Tusla's unique organisational perspective on children's rights, we have identified two additional considerations for the DPC in the context of this consultation. These are presented below.

Child Protection Legislation vs. GDPR

Currently, there appears to exist a degree of uncertainty across organisations regarding the exact circumstances under which child protection may supersede the requirements outlined under GDPR or other relevant data protection legislation. ***Clear guidance from the DPC would be useful to provide clarity in relation to the instances where child protection legislation may supersede the GDPR and other relevant data protection legislation.***

Child Participation in Research

Many policies call for services to be informed by the involvement and participation of children and young people in decisions that affect them. At present, Tusla follows guidance from the Department of Children and Youth Affairs (DCYA) on ethical research with children which states that *"parental/guardian consent is required for a child to participate in research, but good practice also requires the child's agreement/consent*". The HSE National Consent Policy, however, states that *"for the purposes of participation in clinical trials, anyone over the age of 16 years can consent on his/her own behalf. For all other research, the person must be over the age of 18 years in order to provide consent".*

Given the complex policy environment that Tusla operates in, ***additional clarification from the DPC would be beneficial with regard to whether the new digital age of consent will impact the ability of children and young people to give their own consent to participate in research***.

Note: While Tusla does not at present wish to raise any additional issues outside of those above in relation to the subject matter of the consultation, the organisation would be happy to advise on, or assist in, responses to issues raised by any other respondents.

Conclusion

The provisions of the General Data Protection Regulation are complex and multi-faceted, and have introduced a degree of uncertainty for organisations as they navigate the new legislative environment. It is apparent that, even in scenarios related to the personal data of adults, guidance for organisations on the application of the intricacies of the GDPR is required. This need for direction and input from the DPC becomes much more prevalent, and, in Tusla's view, more critical, in the context of the personal data of children.

The best interests of the child have always been paramount to Tusla's organisational and strategic vision, and Tusla welcomes this opportunity to contribute towards the development of effective, well-reasoned guidance materials in relation to the processing of children's data. While the positions and suggestions discussed throughout this document should not be considered comprehensive or definitive, and are intended only as source material for the DPC in the development of its own guidance, it is our hope that some of the key complexities of the GDPR in relation to child protection have been effectively highlighted as a result of this consultation.

Tusla would be happy to accept any additional clarifying questions the Data Protection Commission may have in relation to this consultation document, and to assist in or advise on the development of any guidance materials or regulations resulting from it.