Replies to be sent to childrensconsultation@dataprotection.ie the final date for responses is Friday 1 March 2019.

Feedback to the Data Protection Commissioner

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

Simple systems such as check boxes and FAQ's and simple language-focused to the subject at hand – e.g. if we need personal information such as name and age – why we need them and what we do with them. Posters detailing exactly what information is needed and why could be useful materials to put up in scout dens or libraries or community centres.

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?**

Due to the technical and legal reasons behind GDPR it is a difficult concept to explain even to adults. We aim to be specific with our consent and data protection obligations

On key step is avoiding generic privacy statements in favour of statements relating to the information you are consenting to give.

We also provide sample documents on our site that are already GDPR ready for members to use. E.g. samples of commonly used forms with privacy notices and information about an individual's rights under data protection legislation.

We also have guidelines and a 'how to' document provided for groups and national teams as to their responsibilities and steps they need to take under the new data protection rules.

Furthermore, to help understanding and to reduce the need from members (especially children) to have to read multiple documents we are working on a FAQ page on our site designed to troubleshoot basic questions in clear, simple language for children and adults alike.

We also aim to send out a survey once our broad GDPR strategy has been put in place and check how randomised members felt about different aspects of GDPR, e.g. – did they feel like they knew why we needed the details we were asking them to provide, sample questions below:

-Did they know how long and where their data would be stored?
-Did they know who (and why) we are sharing the data with (if applicable)
-Did they feel sufficiently informed about what they were giving their consent for?

GDPR is a continuous process and we have aimed to create a 'privacy by design system' which is designed to reduce date breaches and misuse of information but also to make the day to day operations GDPR compliant so as to make it part of the system instead of a new task for members to complete.

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?**

We at scouting Ireland would limit the age to 16 – the digital age of consent. Under 18 all personal data is given with the consent of their parent or guardian. The child could still make a SAR through their parents or guardian if they so wished before the age of 16. Under 18 very little date is kept on

any individual, only basic data necessary to the everyday running of our organisation – such as name, date of birth etc. and we operate a strict destruction process on more temporary files such as activity consent forms and managing medications forms.

For a child to be able to make a SAR under the digital age of consent there would have to be extenuating circumstances that involved child protection questions or serious complaints filed.

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?**

   Parents and legal guardians are entitled to submit SARs on their children up until the age of 16. Before that, all data is given and kept with their consent anyway. Between 16-18 parents and children should both consent for the personal data of the child to be released in an SAR.

   The child should be able to make a request for their own data between 16-18 themselves but a notification must be sent to the parents/guardians that a SAR has been requested. The data released is only sent to the child.

   Parents/guardians of child are able to make a SAR on their child provided their child has given consent for them to do so. And the data released will be released to both parties.

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?**

   In cases such as this, unless information has been flagged by the child as 'not to be released' to the parent the data is accessible to both. Obviously where existing legislation kicks in that option does not apply e.g. child protection issues, criminal offenses etc. and the data should be released to the parent as they are legally responsible for the child.

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 digital age of consent is 16. So at 16 years of age a child should be allowed to submit a SAR and an erasure request.

It depends on the type of data – sensitive personal data may be considered for archival importance and therefore is subject to conditions. If the erasure request is deemed to be submitted in order to conceal or obscure information from the parent it should also be deemed subject to conditions.

If SAR or erasure requests are denied under the above mentioned examples a rationale statement, explaining why the decision was taken to refuse the request should be released to the data subject along with a notification about their rights to appeal and judicial process.

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?**

Parents and legal guardians are entitled to submit erasure requests on their children up until the age of 16. Before that, all data is given and kept with their consent anyway. If data is erased a note that this has taken place should be added to the file.

Between 16-18 parents and children should both consent for the personal data of the child to be erased in an erasure request.

The child should be able to make a request for their own data erasure between 16-18 themselves but a notification must be sent to the parents/guardians that an erasure request has been requested.

Parents/guardians of child are able to make an erasure request on behalf of their child provided their child has given consent for them to do so.

Obviously where existing legislation kicks in that option does not apply e.g. child protection issues, criminal offenses etc.

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?**

Date of birth should be used to verify age of participants.
PPS number could also be used to link people to ages within a country
ID number – code on ID card issued - such as the Garda Age card – use the ID number to verify person is over/ under 16. I'm not sure this is currently possible but would be fairly easy to implement.

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?**

   It is very difficult to verify something like this. Perhaps a warning of fines or being blocked/blacklisted from the site for fraudulently claiming to be responsible for the child should appear when parents must give consent. Perhaps a photo must also be submitted (taken as part of the process) of 'parents' giving consent as this would act as a deterrent to people trying to deceive the system and would also act as evidence for the service provider that parental consent was given.

(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?

A 'two step authentication' process is often employed by people to verify their own personal identity when accessing their accounts. Something similar could be applicable in this circumstance. A process such as a digital signature (like the ones employed by the postal service) and or a photo taken as part of the process could be used effectively in this situation.

However that may seem fairly extreme to many so alternatively a second email address belonging to the parent should be supplied during sign up and a digital consent notice supplied. This should be signed/ticked and sent back.

There will always be people who take advantage of the system and with the deeply unregulated nature of the internet we must operate a sort of honour system and do our best with the tools we have.

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?**

They should be re-prompted, as many users will have aged in the time since they signed up. If they are underage they should also be given the chance to sign up again if they provide parental verification or approval. E.g. provide parental email address with a consent release form sent to parental email address. They could also be allowed back on to a restricted version of the site with tight censorship controls and restricts access to all the functions.

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

Look up the law in each country and specify on the landing page for each country. This is easily implemented. GDPR also specifies that the law of the land applies so the age of consent is relative to each country.

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?**

Yes. Marketing profiles can show highly sensitive data that is unique to the data subject and could put them in danger. Children are also highly suggestable and are unable to give informed consent or use adult-level reasoning so it is exploitative to use personal data to target a child for marketing purposes. Any profiles compiled found to be pertaining to children under 16 should be immediately deleted.

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?**

The easiest way to incorporate data protection into organisational systems is to hold the minimum amount of data required (and state exactly why they need it) and uphold a vigorous retention and destruction process, meaning data is only held as long as necessary. This system should also be regularly monitored by a dedicated Data Protection Officer and subject to regular audits and surveys.

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?**

No, if the products or services comply with holding the minimum amount of data possible and destroying it in the specified timeframes it would not be necessary to have tighter controls for

younger children. Within our organisation as a child gets older they are able to interact with more parts of the service, such as national camps and events. These would not be available to a younger member so tightening restrictions would have no effect.

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

There needs to be guidelines put in place concerning redaction of documents released as part of access requests.

Redaction is necessary on many documents subject to access request to protect the data of other people who are not the data subject. Clear rules on what should be redacted should be supplied for ease of organisations completing access requests. Otherwise organisations can incur expensive fees from lawyers or consultants on questions they may have in the process of completing access requests in a lawful and timely manner.