

An Coimisinéir  
Cosanta Sonraí



Data Protection  
Commissioner

## Article

### **The Transparency Challenge:**

Making children aware of their  
data protection rights and the  
risks online

Anna Morgan, Deputy Commissioner – Head of Legal

Originally published in *Communication Law*

The Journal of Computer, Media and Telecommunications Law

Volume 23 No.1 2018 pp 44-48

## Lifting the veil of invisibility

It is timely to focus on children as key stakeholders in the digital ecosystem as we look towards 25 May 2018 and the application of the General Data Protection Regulation<sup>2</sup> (GDPR) across Europe. Post 25 May 2018, for the first time there will be a data protection law at EU level which lifts the veil of invisibility that some would say has hitherto shrouded child users of online and digital services. As recent academic research has highlighted, an estimated one third of internet users across the globe are under 18s.<sup>3</sup> However, as child safety organisations such as the Irish Society for the Prevention of Cruelty to Children have pointed out<sup>4</sup>, these internet users are often operating in a world that was not originally designed with them in mind and still fails to recognise them as key players. However, from 25 May 2018, children are very much at the front and centre of the data protection landscape in Europe. The GDPR attributes special protection to children and so it will shine an unremitting spotlight upon data controllers in relation to safeguarding child users of online services. Effective protection of children in the labyrinthine online and digital environments will involve enabling children to exercise their legal and fundamental rights<sup>5</sup> in a way that minimises the risks to them. This in turn means maximising children's understanding of the cyberterrain they inhabit as a large part of their everyday lives. As Recital 38<sup>6</sup> of the GDPR states: *Children merit specific protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.* Central to that core issue of understandability and awareness is the obligation of transparency upon data controllers under the GDPR.

## Transparency – a reconstructed and recalibrated obligation

Transparency under the GDPR<sup>7</sup> is not so much a brand new concept in the data protection regulatory regime as a reconstructed and recalibrated obligation, albeit one that has now been very much shunted centre stage. Anyone who has ever 'gone online' will be familiar with the concept of privacy policies or privacy statements on websites which data controllers are required to provide as part of the obligation of fair processing of personal data under the current EU law, the 1995 Data Protection Directive.<sup>8</sup> That obligation of fair processing requires certain minimum information to be provided to data subjects, including the fact of their data being processed, why that processing is happening and who the data controller is. However, there has been an enduring apprehension about the utility of that limited information and whether it truly enables data subjects to take control of their personal data. Such apprehension is particularly pertinent in an online context given that privacy policies and statements have traditionally been expressed in lengthy legalistic and specialist terms which can be difficult for the average adult user to understand, let alone comprehensible by child users.<sup>9</sup>

## Regulatory disquietude

The online world with all its permutations is clearly an intrinsic part of children's everyday lives, and it seems that the age at which children start regularly accessing the web is becoming lower and lower. According to Ofcom<sup>10</sup> in a report published in 2016, based on parents' estimates 3-4 year olds are now spending an average of 8 hours and 18 minutes per week online. Arguably, 21<sup>st</sup> century children's use of online services is effectively ubiquitous, with many children now more digitally literate than their parents – sharing photos and videos, sending messages, using social media platforms, playing games and accessing entertainment amongst other activities. The issue of transparency in services targeted at children has long been a topic of global concern in the data protection sphere. The International Conference of Data Protection and Privacy Commissioners has issued a number of resolutions<sup>11</sup> in recent years addressing children's online privacy and the need for educational initiatives, and ventilating disquietude about the online encroachment into the private lives of children and the fact that children are often unaware that their information, habits and behaviour are being tracked online. Such regulatory anxiety was arguably validated by the results of the Global Privacy Enforcement Network Privacy Sweep of 2015<sup>12</sup> which saw 29 data protection regulators around the world, including the Irish Data Protection Commissioner and the Information Commissioner's Office in the UK, examine a total of 1,494 websites and apps which were targeted at, or popular amongst, children. The results raised concerns particularly around the volume of children's personal information that was collected by those websites and apps, and later shared with third parties. Among its findings, the study revealed that while 67 per cent of the sites and apps examined collected children's personal data, only 22 per cent tailored their data protection communications to children.

## ‘Children merit specific protection’<sup>13</sup>

The understandability gap in information that data controllers must provide to individuals, particularly where those individuals are children, is what the newly enunciated transparency obligation under the GDPR seeks to address. The core transparency obligation is found in Article 12<sup>14</sup> of the GDPR, with Article 12.1 requiring data controllers to take appropriate measures to provide the required information, related to processing of personal data, to data subjects in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The specific information that must be provided by the data controller to a data subject is now extensive (in comparison with the equivalent information requirements applicable under Articles 10 and 11<sup>15</sup> of the 1995 Data Protection Directive) and is set out in Articles 13<sup>16</sup> and 14<sup>17</sup>. It includes information about who the data controller is, how the personal data will be used, who it will be shared with, whether it will be transferred internationally, the period for which it will be stored, and very importantly, what the data subject’s rights are – for example, the right to access, rectification, and erasure of personal data and to make a complaint with a data protection authority. Insofar as providing information to and communicating with children is concerned, it is hugely significant that Article 12.1 of the GDPR carves out an explicit transparency obligation on data controllers for any information which is ‘addressed specifically to a child’.<sup>18</sup> This ties in with Recital 58<sup>19</sup> of the GDPR, which makes it clear that because children merit specific protection, any information and communication concerning the processing of a child’s data ‘should be in such a clear and plain language that the child can easily understand’.

## Appropriate measures to achieve transparency

So, what does this new GDPR transparency obligation mean in practical terms for data controllers, such as the tech giants that run the social media, gaming, messaging and photo-sharing websites and apps that are so popular with children? The answer to this is bound up in one of the most important phrases in Article 12, namely the requirement in Article 12.1<sup>20</sup> that data controllers take ‘appropriate measures’ to provide the required information to data subjects in a concise, transparent, intelligible and easily accessible form. According to Article 12.1, such information is to be provided in writing, or by other means, including where appropriate, by electronic means. However, the term ‘appropriate measures’ clearly does not provide a fixed benchmark for all data controllers. Instead, it denotes an inherent variability depending on the circumstances in which the data controller is processing personal data. Fundamental to a data controller’s ability to comply with the obligation to take ‘appropriate measures’ to convey the necessary information to a data subject is that the data controller must first know their audience and then tailor the communication of the information to data subjects in a way that is appropriate to that audience. Therefore, if a data controller knows (as it should do) that its audience consists of, or includes, child users, then it should tailor its privacy information and communications so that child users can readily understand what is happening to their personal data and what their rights are. This necessitates the data controller assessing what the most effective modality will be for conveying the information required under Articles 13 and 14 of the GDPR. Such an assessment may include a consideration of the content and accessibility of written statements, as well as the potential use of more visually based techniques such as cartoons, pictograms, infograms and videos. It should also involve an evaluation of the appropriateness of electronic tools such as layered information notices, pop-up notices, hover-over notices or voice alerts. Of course, central to such considerations is the type of device that is being used, and whether, for example, the device is a tablet, mobile phone or an internet-of-things device (including so-called ‘smart’ toys). Whatever the device, it is essential that the measures chosen for conveying the information are appropriate to the device being used by the child. With written statements, the overriding requirement for clear and plain language means that privacy notices that are addressed to child users, or users including children, must employ a vocabulary, tone and style of the language that is appropriate to and resonates with children. This necessarily means no ‘legalese’, no technical terms, jargon or ambiguous phrases that are devoid of any real meaning and may be particularly difficult for children to understand.

## The biggest transparency challenge of all?

However, the data protection transparency challenge is not simply about ensuring data controller organisations provide information and communicate in ways that children can understand. Privacy education is essential to encouraging an awareness amongst children of what their personal data is, what their rights are and what the risks are when they share their information online or digitally.<sup>21</sup> No matter how accessibly or appealingly privacy information is presented on a website or an app used by children, if child users do not appreciate the significance of what that information is telling them, then the risk is that they will swipe right past it without taking any notice of it. So perhaps the biggest transparency challenge is getting children to *want* to understand how and why their personal data is used and processed. That challenge has to be embraced not only by data controllers but also by data protection authorities, policy makers, educators, and parents who all have vital roles to play when it comes to educating children and young people about their rights and risks online. The UK Children's Commissioner, in the 'Growing Up Digital' taskforce report<sup>22</sup> in January 2017, called for the creation of a digital citizenship programme to be compulsory in every school from the age of 4 to 14. Similar sentiments were echoed recently in submissions<sup>23</sup> made to an Irish Parliamentary Committee on Children and Youth Affairs in the context of its examination of cyber security for children and young adults. Indeed, digital literacy is already a focus of many educational programmes but in addition to taking account of the more high profile risks around issues like cyber bullying and general online harassment which attract much attention, children also need to be educated about the perhaps more oblique risks arising from their personal data being collected in the digital ecosystem.<sup>24</sup> Awareness of the right to transparency in personal data processing is growing, and societally it seems that there is movement in the right direction, particularly with the incoming GDPR obligations on transparency. However, arguably technology is currently winning the race over transparency in the privacy arena. There is still a lot of catching up to do in fostering a culture where children – and indeed adults – expect and seek out transparent information from those organisations who collect, use and profit from personal data<sup>25</sup> so that children, and adults, can make smart, informed choices about how, and when, and to what extent, they chose to share their most invaluable asset – their personal data.

**Anna Morgan The author is a solicitor and Deputy Commissioner (Head of Legal) with the Data Protection Commissioner for Ireland. She is the lead rapporteur for the Article 29 Working Party Guidelines on Transparency under the GDPR. This document has been prepared by the author solely for presentation and discussion purposes. Its contents do not constitute legal advice and are not intended to be relied upon by any party as legal advice, nor should they be taken as representing the position or views of the Data Protection Commissioner for Ireland on any matter.**

This paper was presented by the author at the Institute of Advanced Legal Studies Information Law and Policy Centre Annual Conference 2017, the theme of which was 'Children and Digital Rights: Regulating Freedoms and Safeguards'. 2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Dir 95/46/EC (General Data Protection Regulation). 3 Sonia Livingstone, John Carr and Jasmina Byrne, 'One in Three: Internet Governance and Children's Rights', Innocenti Discussion Paper No 2016-01 (UNICEF Office of Research, Florence, 2016) 10. 4 See, for example, the ISPC leaflet 'Cyber safety is the child protection issue of our time' tweeted by the ISPC (@ISPCChildline) on 25 October 2017. 5 The right to Respect for Private and Family Life (Art 7) and the right to Protection of Personal Data (Art 8) are fundamental rights under the Charter of Fundamental Rights of the European Union. 6 Recital 38 of the General Data Protection Regulation: 'Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.' 7 The Article 29 Working Party has published Guidelines on Transparency under the GDPR, a final version of which will be issued following the conclusion of a public consultation (running until 23 January 2018) on the guidelines: [http://ec.europa.eu/newsroom/article29/news.cfm?item\\_type=1310&tpa\\_id=6936](http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1310&tpa_id=6936) 8 See Art 10 (Information in cases of collection of data from the data subject) of Dir 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 9 See, for example, the Article 29 Working Party Opinion 10/2004 on More Harmonised Information Provisions at p 5, para 4. 10 'Children and parents: media use and attitudes report' (Ofcom, 2016), p 47, fig 17. 11 30<sup>th</sup> International Conference of Data Protection and Privacy Commissioners (2008, Strasbourg), 'Resolution on Children's Online Privacy'. 38<sup>th</sup> International Conference of Data Protection and Privacy Commissioners (2016, Marrakesh), 'Resolution for the Adoption of an International Competency Framework on Privacy Education'. 12 For more information on the results of the 2015 Global Privacy Enforcement Network Privacy (GPEN) sweep, see the GPEN 2015 Annual Report. <https://www.privacyenforcement.net/sites/default/files/Annual%20Report%20Final%20Version.pdf> and also <https://www.dataprotection.ie/documents/GPen/GPEN2015.pdf> 13 Recital 38. The principle is also referred to in Recital 58 of the GDPR, as considered further below. 14 Article 12 of the GDPR: Transparent information, communication and modalities for the exercise of the rights of the data subject. 15 Article 10: Information in cases of collection of data from the data subject) and Art 11: Information where the data have not been obtained from the data subject. 16 Article 13 of the GDPR: Information to be provided where personal data are collected from the data subject. 17 Article 14 of the GDPR: Information to be provided where personal data have not been obtained from the data subject. 18 Article 12.1 states: 'The controller shall take *appropriate measures* to provide any information referred to in Arts 13 and 14 and any communication under Arts 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, *in particular for any information addressed specifically to a child*. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means' (emphasis added). 19 Recital 58 states: 'The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.' 20 See n 18 above. 21 See, for example, the International Conference of Data Protection and Privacy Commissioners, 'Personal Data Protection Competency Framework for School Students' (October 2016), p4: 'In the digital age, responsible, ethical and civic-minded education in the use of new technologies is a priority for action, particularly young people in school. A key component of digital education is highlighting privacy and personal data protection. Educators have a key role to play in this digital education of citizens': [https://edps.europa.eu/sites/edp/files/publication/16-10-18\\_resolution-competency-framework\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/16-10-18_resolution-competency-framework_en.pdf). 22 Children's Commissioner, 'Growing Up Digital: A report of the Growing Up Digital Taskforce' (January 2017), p3: [https://www.childrenscommissioner.gov.uk/wp-content/uploads/2017/06/Growing-Up-Digital-Taskforce-Report-January-2017\\_0.pdf](https://www.childrenscommissioner.gov.uk/wp-content/uploads/2017/06/Growing-Up-Digital-Taskforce-Report-January-2017_0.pdf) 23 Submissions to the Joint Oireachtas Committee on Children and Youth Affairs can be accessed under September 2017 and October 2017 at: [http://www.oireachtas.ie/parliament/oireachtasbusiness/committees\\_list/cya/presentations/](http://www.oireachtas.ie/parliament/oireachtasbusiness/committees_list/cya/presentations/) 24 As illustrated, for example, by dialogue with children recorded by the 5Rights movement at: <http://5rightsframework.com/the-5-rights/5rights-by-young-people.html> 25 See, for example, p 22 of the Better Internet For Kids Roundtable Report (June 2016) on 'The General Data Protection Regulation and children's rights: questions and answers for legislators, DPAs, industry, education, stakeholders and civil society': [https://www.betterinternetforkids.eu/documents/167024/2013511/GDPRRoundtable\\_June2017\\_FullReport.pdf/e6998eb6-ba3c-4b5d-a2a6-145e2af594f2](https://www.betterinternetforkids.eu/documents/167024/2013511/GDPRRoundtable_June2017_FullReport.pdf/e6998eb6-ba3c-4b5d-a2a6-145e2af594f2)