

Transparency: an overlooked tool that empowers children

By Ayca Atabey

Transparency is key to designing an online world where children's needs and their best interests are the priority. It empowers children because only when children know about their rights, can they act on them.

Providing information is not enough. Organisations must make sure that they integrate transparency into their business practices and enable children to exercise their rights through design of their services. Implementing child-friendly transparency measures and policies is essential because, as **Recital 38** GDPR provides:

“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.”

The Age-Appropriate Design Code (the Code)¹, the first of its kind in the world to take into account the UN Convention on the Rights of the Child (UNCRC), includes a **transparency standard** that supports compliance with **the transparency principle**² – one of the bedrock principles in **Article 5(1)(a)** (“**lawfulness, fairness and transparency**”) – of the UK General Data Protection Regulation (UK-GDPR).



Photo by April Bryant, from Pixabay

What the law says about transparency

The transparency principle (Article 5(1)(a)) requires data controllers to be clear, open and honest about what they do with and how they use people's data. It is linked to the right to be informed and the right of access to their data, which empower people by giving them more control over their data. The transparency principle is further developed in other parts of the UK-GDPR³.

Transparency rules under the UK-GDPR pay particular attention to the needs of children. For example, Article 12(1) provides specific protection for children and says that the required information (including information about their rights) should be communicated:

“...in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child...”

Recital 58 says that information given to children should **make it easy for them to understand** what data are processed about them and for what purposes they will be used. The Information Commissioner’s Office’s Guide confirms that when processing children’s data, particular care is needed to give **information in a clear and plain language**. Similarly, Guidelines on Transparency published by Article 29 Working Party explains that **the vocabulary, tone, and style of the language used should be appropriate to children**.

The above rules mean that **privacy policies must be tailored to children’s needs**, be child-friendly and make it easy for children to understand what will happen to their data, what rights they have, and how they can exercise these rights.

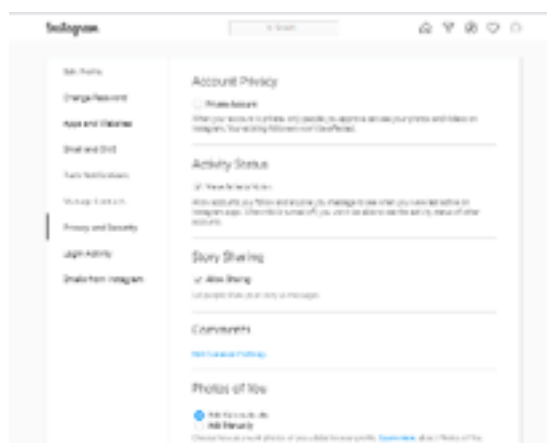
What happens in practice?

Despite the fact that the UK-GDPR provides child-centred rules, there seems to be a gap between what the transparency rules require and what happens in practice. For example, WhatsApp, Instagram, Among Us, Minecraft, Fortnite, and many other online services don’t provide a separate privacy policy or explanation for children as required under the Code.

Privacy policies are generally lengthy, and the format, language and representation of the information is **no different than the one provided for adults**. In other words, **privacy policies are not tailored according to the needs of children**. There is no summary, nor a bite-sized approach as recommended in the Code.

The Code states that privacy policies can include diagrams, cartoons, graphics, video/audio and gamified or interactive content that can be interesting for children, rather than merely being text-based. However, privacy policies are generally only text based. They don’t use icons or visualisation as indicated by the UK-GDPR or provide any tools and mechanisms that help presenting information in a way that is likely to appeal to children.

For example, upon signing up for a new account, Instagram currently sets children’s account “public” by default and gives no information telling children that the account the child has created is public. This is clearly against both the text and the spirit of the transparency rules, which aim to give children control over the use of their data and protect their best interests.



Default settings upon creating an account.

On the other hand, following the introduction of the Code, some companies are making efforts to tighten their privacy policies and take children's best interests into account in their business practices. For instance, TikTok's recent announcement shows impact of the Code as the company stated that there will be significant changes aimed at increasing protections for children. Under the new measures, **all TikTok users under the age of 16 will have their account set to private as default.**

In general, the current practices seem to assume that children are able to read all the information provided in privacy policies made for adults. This approach is not inclusive and undermines children's rights to data protection and privacy. Failing to make information accessible to children arguably means indirectly discriminating against children based on their "age". This is because although children have the same rights as adults, they are not provided the same information and opportunities to exercise their rights.

What should happen now

Transparency rules under the UK-GDPR are not age-blind. Both the law and its interpretation by Information Commissioner's Office make it very clear that **children deserve additional care and organisations must reflect children's needs when communicating information to children.** Yet, generally, the privacy policies of the most popular online services among children do not fully reflect the needs of the online world, where one in three users are children. With children's best interests in mind, the child-centred transparency rules should be urgently implemented in practice. Aligned with the transparency standard of the Code, adopting an age-appropriate and need-based approach in privacy policies would benefit organisations by showing compliance with the transparency rules and putting them in a better position as regards respecting children's rights.

Notes:

[1] The Code covers online services (like social media, connected toys/devices) that are likely to be accessed by children in the UK and that process their personal data. It helps online services to design services that comply with the General Data Protection Regulation (GDPR) and the Privacy and Electronic Communications Regulations (PECR).

[2] Note that transparency principle is set out under Article 5(1)(a) and explained in Recital 39, requiring individuals be made aware, in a form "easily accessible and easy to understand," that "personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed".

[3] Transparency principle is further embedded and developed in other parts of the GDPR (e.g., Articles 12-14, 34).

This blog is part of the innovation series. You can view the rest of the blog series here.

Ayça Atabey is a lawyer and a researcher, currently enrolled as a PhD student at Edinburgh University. She has an LLM (IT Law) degree from Istanbul Bilgi University and an LLB (Law) degree from Durham University. Her PhD research focuses on the role that the notion of 'fairness' plays in the protection of vulnerable data subjects. Her

work particularly involves the intersection between data protection, information privacy, and human rights issues. She is a research assistant for the Digital Futures Commission. Prior to this, she worked as a lawyer in an international law firm and has been working as a researcher at the BILGI IT Law Institute.



Originally posted on <https://digitalfuturescommission.org.uk/> on June 7, 2021 .