Data protection in children's best interests: what's at stake?

By Ayça Atabey

How can children's best interests be addressed through data protection? The Digital Futures Commission works towards embedding children's best interests in the design of the digital world, in which data and their usage are of paramount importance. Of importance to our work is the Age-Appropriate Design Code (the Code), the first of its kind in the world to take into account the UN Convention on the Rights of the Child (UNCRC).

The Code sets 15 standards for providers of information society services (online services such as social media platforms, apps, games, connected toys/devices) that are likely to be accessed by children in the UK and that process their personal data. It supports compliance with data protection principles (Article 5 of the UK-GDPR)[2] through specific protections aligned with Article 25 (Data Protection by Design and by Default) of the UK General Data Protection Regulation (UK-GDPR). This requires **data controllers** to ensure they have appropriate and effective data protection by design and by default.

Article 25 addresses data **controllers**. However, the Information Commissioner's Office's Guide explains that it would be wise for **any organisation** (e.g., **processors** and **other parties** such as app developers/manufacturers) to keep data protection by design and by default in mind when processing data or designing products/services. This is because Article 28 says controllers must use **processors** providing sufficient guarantees to meet the UK-GDPR's requirements and Recital 78 extends data protection by design to other organisations. Therefore, even though organisations other than controllers are not directly obliged to comply, adhering to data protection by design and by default rules would put them in a better position in their business practices and in respecting children's rights.

Note that the Code helps online services to design services that comply with the General Data Protection Regulation (GDPR) and the Privacy and Electronic Communications Regulations (PECR).

B. Flickinger

What do we mean by "Data Protection by Design and by Default"?

- ***"Data protection by design"* (Article 25(1))** means embedding privacy and data protection principles (Article 5) into the design of processing operations starting from an early stage right through the lifecycle of product development. The Information Commissioner's Office refers to *"data protection by design"* as baking in data protection into the very design of processing activities and business practices.
- ***"Data protection by default"* (Article 25(2))** means ensuring personal data are processed with the highest privacy protection. User service/product settings must be data-protection friendly by default, and that only data necessary for each specific purpose should be processed in accordance with data protection principles (Article 5), particularly data minimisation and purpose limitation.

Good practice examples would include having privacy settings set to high by default, having behavioural advertising switched off by default or privacy settings that make it easier for children to exercise their rights under UK-GDPR (such as the rights to access or erasure).

Why is "Data Protection by Design and by Default" so important?

From a children's rights perspective, data protection by design and by default (Article 25) is essential for the protection of children's rights because,as Recital 38 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.*"

Due to their vulnerable nature, children rely significantly on the protection provided by Article 25. Therefore, products/services must be designed by considering vulnerabilities, needs, and fundamental rights and freedoms of children by design and default.

Despite this necessity, there seems to be a gap between what the law says and what happens in practice. 5Rights' submission to the European Data Protection Board highlights how current practices overlook the needs of children and undermine their rights. 5Rights' Disrupted Childhood report explains how privacy concerns are overlooked in the design processes and the persuasive design techniques are used to nudge children towards decisions that increase their engagement while reducing their privacy.

How the Age-Appropriate Design Code helps

All 15 standards of the Code are closely linked to relevant data protection principles, particularly the fairness principle, which should be at the heart of all processing activities involving children's data. The principles aim to protect the people's interests and this is particularly important where children are concerned. The Code provides the specific protections children require for their data, by design and by default and gives some practical examples on their implementation under *"data minimisation"* and *"default settings"* standards.

Aligned with Article 25, the Code sets high-privacy default settings standard. Like any service that is likely to be accessed by a child, connected toys or devices' settings must be 'high privacy' by default. The exception to this rule is if organisations can show a compelling reason for a different default setting, taking into account the child's best interests, on a case by case basis. Determining the best interests of the child is a balancing act between different rights and freedoms which requires a good understanding of children's rights.

Livingstone and Pothong underscore the importance of Child Rights Impact Assessment as a tool for realising the best interests of the child in relation to the digital environment and conclude that

> "*it offers clarity of vision, a strong rationale for action and it integrates the multiple calls for better privacy, safety, security and ethics-by-design in a single framework*".

Equality by design: A missing link

Knowing some children are more vulnerable than others, compliance with Article 25 also needs services to be designed in line with the different ages and vulnerabilities of the children likely to access them. This inclusive approach is supported by the Code, which addresses the need to consider the relevant equality legislation in the UK (e.g., Equality Act 2010). To do this, companies must consider how such vulnerabilities can affect children's rights and how they can be mitigated by putting the Code in practice in compliance with data protection by design and by default (Article 25).

With children's lives now digital by default because of the COVID-19 pandemic, the need to take action to firmly implement data protection by design and by default (Article 25) requirements with children in mind has become more urgent than ever. We need robust legal and practical frameworks reflecting the needs of the online world, where one in three of the users are children. Prioritising children's best interests and understanding the enabling role that "data protection design and by default" (Article 25)[1] play in protecting their rights under the UK-GDPR are good starting points.

Although the Code sheds some light on how to apply data protection by design and by default in practice by taking children's rights into account, more is needed to help online services understand the practical implications of *each principle* and *the requirements* of Article 25. We invite regulators to provide more practical guidance with specific

case studies from different industries (EdTech, online gaming). We also invite digital providers to make the best interests of the child "the paramount consideration" in the design and development of their data systems and their processing of children's data.

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

Notes for reader:

- Note that the Code helps online services to design services that comply with the General Data Protection Regulation (GDPR) and the Privacy and Electronic Communications Regulations (PECR).
- Note that The Code`s role in supporting compliance with Article 5 is crucial in enhancing children`s data protection rights. This is because the core data protection principles lie at the heart of the UK GDPR. They are set forth at the beginning of the legislation and inform everything that follows. Therefore, compliance with these principles and their effective implementation as required under Article 25 (Data Protection by Design and by Default) is vital for protecting individual rights of the UK GDPR.
- Article 28 asks controllers to only use processors that provide "sufficient guarantees to implement appropriate technical and organisational measures" to meet the requirements. Moreover, (without compliance requirements) Recital 78 encourages producers (e.g., product designers/app developers) to take into account the right to data protection so that controllers and processors are able meet their data protection obligations (e.g., designing a product in a way that enables controllers to comply with their data protection by design and by default requirements). This is why taking rules for data protection by design and by default into account when designing products/services would give a company a competitive advantage in the market as controllers would be more willing to do business with such companies.
- Note that Article 25 (data protection by design and by default) is an enabler for effective application of Article 5 (data protection principles) as it requires to implement measures that are designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing to meet the requirements of the UK-GDPR and protect data subjects` rights. This is important because Article 5 (data protection principles) lie at the heart of the UK-GDPR and is an enabler for data subjects` rights.

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.