


Children's personal data: Retailers beware of new regulatory changes

10 February 2025  Francis Katamba and Conor Moran

In the evolving landscape of digital commerce, the processing of children's personal data is a hugely complex and sensitive issue which is now subject to increased regulatory scrutiny.

With aspects of the Online Safety Act 2023 in the UK set to come into effect from 16 March 2025, alongside a host of relevant regulation in the fields of data protection, AI, and consumer protection, it is crucial for organisations in the retail sector to stay informed and compliant. This is particularly important if your online services allow any user-to-user interaction and content posting.

What is the key issue for retailers?

Regardless of whether you are intentionally targeting children with advertising and inviting them to engage in online purchases, or whether children use your online services without express targeting, you will be subject to a complex regulatory landscape.

Many clients we work with are unaware of the sheer scope of regulation in this space in relation to the processing of children's data in the areas of online activity, and any marketing, advertising and profiling. Due to the extensive regulatory changes in this landscape, it can be difficult for organisations to adopt a proactive approach to pre-empt potential challenges and risks with increased regulatory scrutiny.

It is vitally important for retailers to take a step back to consider the potential regulatory risks, and the consequential business harms that could be associated with regulatory intervention in relation to the processing of children's personal data. There is also a potential for significant regulatory fines in this space given the increased regulatory focus, not to mention the reputational damage that a retailer could suffer if subject to regulatory scrutiny.

The legal framework

The EU's General Data Protection Regulation (GDPR), and its UK counterpart (UK GDPR), highlight the need for specific protection of children's personal data, especially concerning profiling. The Information Commissioner's Office (ICO) has developed a comprehensive Children's Code to guide online services on age-appropriate design principles. This code outlines 15 standards, emphasising the importance of transparent, child-friendly privacy information and prioritising the child's best interests during data processing.

As noted above, the Online Safety Act 2023 also ushers in a new era of digital regulation focused on minimising online harms and increasing online safety.

This flurry of regulatory change also includes the EU AI Act which will directly or indirectly impact many organisations. Since 2 February 2025, "any exploitation of vulnerabilities of individuals due to age, disability, or social or economic situation" is now officially a prohibited AI practice under the EU AI Act.

The Data Use and Access Bill (DUA Bill) also appears likely to pass through the UK Parliament relatively smoothly and will result in further changes to the data compliance landscape in the UK.

Profiling and marketing to children

Profiling children for marketing purposes, particularly in high-value sectors, is a contentious area. Although not explicitly prohibited, the GDPR recitals advise caution and suggest that such activities should generally be avoided due to the vulnerability of this demographic. This is also reflected in the regulatory focus in the EU AI Act on any AI practices that target any vulnerabilities of individuals based on age.

Retailers often state in their policies that they do not intend to process the personal data of children, however in practice it can be very difficult for organisations to ensure this without implementing potentially expensive safeguards such as age verification software.

A pragmatic, risk-based approach may be needed to manage these risks proportionately. And retailers who do engage in profiling or marketing which may involve the processing of children's personal data should be careful to make sure that they understand any risks involved and have taken appropriate steps to mitigate them.

Practical steps for retailers to take

We often see retailers dealing with issues such as the processing of children's personal data reactively following the manifesting of a risk which had not been fully appreciated, or a change in the law which they had not addressed.

We would encourage retailers to take a step back and proactively assess how to manage these risks as part of a wider governance, risk and compliance strategy. This should support their overarching data governance framework and align with their management of enterprise risk.

Whilst this can seem daunting there are some practical steps retailers can take to help them deal with the complex and evolving regulatory landscape:

1. Data mapping

It is essential to set aside some time to take stock and map the organisation's data flows to understand use of personal data in the business. Organisations should undertake a comprehensive data mapping exercise to understand how children's data is processed and why. The core aim of this should be to assess the potential risks in light of the recent regulatory changes and increased scrutiny to align the organisation's approach to their risk profile.

2. Impact assessments

Organisations should conduct Data Protection Impact Assessments to evaluate risks and mitigation strategies when processing children's data, particularly for profiling and marketing.

3. Adherence to the ICO's Children's Code

It is vitally important to ensure all practices comply with the ICO's Children's Code, focusing on transparency, the child's best interests, and privacy by design.

4. Privacy notice design

Retailers should design privacy notices that are easily understandable by children, using clear language and presenting information at key interaction points. When drafting privacy notices, clarity and accessibility are paramount. Retailers should consider implementing child-friendly privacy notices that are concise and presented at relevant interaction points, such as account creation. A layered approach to privacy notices can also further enhance understanding and accessibility for both children and their guardians.

Conclusion

It is important that retailers stay abreast of this area of regulation and proactively manage their legal risks while fostering a safe and responsible online environment for all users. As well as avoiding fines and litigation this may also build trust with their stakeholders and help strengthen their brand.

Contact

Francis Katamba



Partner

francis.katamba@brownejacobson.com

+44 (0)330 045 2725

Conor Moran

Associate

conor.moran@brownejacobson.com

+44 (0)330 045 2926

Related expertise

Advertising and marketing

Consumer and e-commerce

Data protection and privacy

Data protection for retail