KEYSTONE LAW

CHILDREN'S PRIVACY ENFORCEMENT INTENSIFIES: LESSONS FROM ICO'S REDDIT AND IMGUR DECISIONS

Two recent enforcement decisions from the UK Information Commissioner's Office (ICO) provide a clear signal about the regulator's priorities for online platforms. In February 2026, the ICO imposed a £14.47 million fine on Reddit (a well-known user-curated news and discussion platform) and a £247,590 fine on MediaLab, the owner of Imgur (an image hosting and sharing service, designed for easily sharing photos, GIFs, and memes online). Both decisions concern failures to protect children's personal data on online platforms.

The cases show that the ICO is tightening scrutiny of platforms likely to be accessed by children, with particular attention to age assurance mechanisms and compliance with the UK's children-specific data protection framework.

For online platforms and digital services, the decisions provide several practical insights.

KEY TAKEAWAYS:

- The inadequacy of self-declared age gates, particularly for platforms with user interaction and user-generated content.
- The convergence of regulatory regimes governing child safety online.
- The realistic possibility that a compliance issue identified by one regulator could trigger scrutiny from another.
- How an effective Data Protection Impact Assessment (DPIA) can mitigate fines, while a broader compliance strategy can help businesses successfully navigate overlapping legal frameworks.
- How a service views itself may not necessarily be how the regulators view it as forum-based or community platforms are increasingly regarded as social platforms with corresponding responsibilities.

1. OPERATIONALISING THE CHILDREN'S CODE

Both decisions centre on the UK's **Age Appropriate Design Code**, often referred to as the Children's Code. The Code, issued by the ICO under the Data Protection Act 2018 and the UK General Data Protection Regulation, translates general data-protection principles into **15 design standards for online services likely to be accessed by children**.

At its core, the Code requires organisations to place **the best interests of the child at the centre of service design**, including through privacy-protective defaults, appropriate data minimisation, and robust risk assessments.

The Reddit and Imgur decisions illustrate how the ICO is enforcing these standards in practice.

In both cases, the ICO found two central failings:

- **No lawful basis for processing personal data of children under 13**. Under UK law, online information services may only rely on consent for processing the personal data of children under 13 if parental consent has been obtained. Both platforms processed children's data without such consent or another valid legal basis.
- **Failure to conduct a Data Protection Impact Assessment (DPIA)**. The ICO concluded that the companies had not carried out a DPIA addressing the risks posed to children, even though their services were accessible to users under 18.

The ICO emphasised that the absence of risk assessment meant the platforms had not properly considered how children's data could expose them to harmful or inappropriate content.

2. HOW CHILDREN ACCESS PLATFORMS WITH SOCIAL FEATURES

A central theme in both decisions is the inadequacy of **self-declared age gates**, particularly for platforms with user interaction and user-generated content.

In the Reddit case, the platform prohibited users under 13 in its terms of service, yet the ICO found that it had **no effective mechanism to verify users' ages until July 2025**. As a result, under-13 users were able to access the platform, and their personal data was processed without a lawful basis. Imgur presented a similar issue: users could access the service without meaningful age checks despite the platform hosting user-generated content and processing personal data.

The ICO was explicit that **simply asking users to declare their age is insufficient where children are likely to access the service**. At the same time, the decision highlights a persistent compliance tension: stronger age verification often requires collecting additional personal data, while data protection law emphasises data minimisation. The regulator nevertheless expects platforms to implement **age assurance measures that are proportionate to the risks of the service**.

3. INCREASING REGULATORY CONVERGENCE IN THE UK

These cases also illustrate **the convergence of regulatory regimes governing children's safety online**.

In the UK, children's online protection is now addressed through two key overlapping frameworks:

- data protection law and the Children's Code, enforced by the ICO
- online-harm regulation under the Online Safety Act 2023, enforced by Ofcom

Although these regimes have different legal bases, the regulators are increasingly focusing on similar risks. Both frameworks require companies to consider whether children are likely to access the service; the risk of exposure to harmful or inappropriate content; risk assessments and mitigation measures; and effective age-assurance mechanisms.

The ICO has explicitly stated that it is working closely with Ofcom to coordinate regulatory oversight. For businesses, this creates a realistic possibility that **a compliance issue identified by one regulator could trigger scrutiny from another**.

4. PARALLEL TRENDS IN THE EUROPEAN UNION

Although these decisions arise under UK law, the regulatory logic closely mirrors developments in the European Union.

Under the General Data Protection Regulation (***GDPR***), children's data also receives enhanced protection, and parental consent is required for younger users. Meanwhile, the Digital Services Act (***DSA***) requires platforms to assess and mitigate systemic risks affecting minors, including exposure to harmful content and the design of recommender systems.

As a result, the UK and EU frameworks are converging around similar expectations such as risk-based design for services likely to be accessed by minors; documented impact assessments; stronger safeguards for children's personal data; and meaningful age assurance mechanisms.

5. RISK ASSESSMENTS AS FOUNDATION OF COMPLIANCE

Both ICO decisions also illustrate how **risk assessments and DPIAs can serve as a critical compliance safeguard**. Under the UK Children's Code, as well as broader UK (and EU) GDPR obligations, platforms that are likely to be accessed by children are expected to assess and document risks to minors. In practice, such assessments are often the primary evidence that an organisation has identified potential harms and implemented proportionate safeguards. Both Reddit and Medialab could have seriously reduced their fines if they had conducted a DPIA.

More broadly, the regulatory framework governing children online has become increasingly complex. Online services must navigate the Children's Code, guidance under the Online Safety Act, and parallel requirements emerging under EU instruments such as the GDPR and the DSA.

KEYSTONE LAW

The challenge for organisations is therefore less the absence of guidance than **the need to map and align these overlapping obligations**.

The cases also show that enforcement is directed particularly at services with **social or community features**, broadly understood. Platforms built around user interaction, messaging, or content sharing fall squarely within the ICO's priorities. Importantly, a service does not need to view itself as a traditional social network to be treated as such. Reddit's treatment shows that forum-based or community platforms are increasingly regarded as **social platforms with corresponding responsibilities**.

For companies operating across both jurisdictions, a **single compliance strategy addressing children's risks across data protection and platform regulation** will likely become necessary.

Importantly, the exercise should not remain confined to legal or compliance teams. Conducting a DPIA can create a structured dialogue between **compliance, safety, product and engineering teams**, helping organisations identify risks early and design appropriate safeguards. In addition to reducing regulatory exposure, this approach can strengthen user trust – an increasingly valuable asset as public scrutiny of online safety grows.

FOR FURTHER INFORMATION

REIGN LEE
Partner
T. +44 (0)20 3319 3700
M: +44 (0)7724 516 153
E. reign.lee@keystonelaw.co.uk

THIBAUT D'HULST
Partner
T. +44 (0)20 3319 3700
M: +32 478 200 944
E. thibaut.dhulst@keystonelaw.co.uk

DIGITAL COUNSELLING PRACTICE

Holistic. Strategic. Impactful.

Keystone Law's Digital Counselling Practice delivers practical, scalable guidance rooted in what businesses can actually do, not just legal theory. We focus on what's workable, commercial and forward-looking.

HOW WE CAN HELP YOU

- **Legal Strategy Review:** We identify compliance gaps, risks, and liabilities in your digital operations and help you optimise your legal position.
- **Business-Legal Alignment:** We embed design thinking into your digital strategy to support innovation, commercial priorities and reduce friction.
- **Governance Support:** We build legal and compliance frameworks to guide policy, risk, and accountability in digital initiatives.
- **Regulatory Readiness:** We help you stay ahead of legal developments with proactive policies and audits.
- **Ongoing Support:** Provided on-call counsel to address evolving issues in digital regulation and international compliance.

IS YOUR STRATEGY FUTURE-PROOF?

From product design to data workflows, marketing practices to compliance frameworks, we help you spot risks early, stay ahead of regulations, and align legal strategy with business growth. Whether you're scaling, innovating, or just trying to keep up - we've got your legal foundation covered.

Let's make your digital transformation legally sound. Talk to us today.