PRIVACY & DATA PROTECTION VOLUME 26, ISSUE 4

Navigating compliance with children's data protection requirements in the EU and UK

Jonathan Wright, Partner
Ashley Webber, Associate
Hunton

Jonathan Wright, Partner, and Ashley Webber, Associate, Hunton, explore some of the key compliance principles for processing children's data online, providing practical examples of ways to comply with such principles

Over recent years, data protection as it applies to children has been a topic of significant consideration globally. In the EU and UK, following the introduction of the EU General Data Protection Regulation (the 'GDPR', references to which shall also include the UK GDPR) in 2018, which included relatively few obligations specifically related to children, we have seen data protection regulators take a keen interest in children's data, issuing guidance, launching investigations, and, in certain instances, taking enforcement action. What is clear from this regulatory focus is that children's data protection is no longer a niche confined to child-directed services, but a broader governance and risk consideration for any online service that may be accessed by children. However, even with such guidance, many organisations that process children's data consider compliance a challenge, often finding it difficult to adapt their existing data protection programmes so that they are suitable for children. This article looks to explore some of the key compliance principles for processing children's data online, providing practical examples of ways to comply with such principles, drawing on the guidance of EU and UK data protection regulators.

When is an organisation processing children's data online?

The GDPR does not provide a test for when an organisation is deemed to be processing children's data. However, EU and UK regulators have established tests through their guidance which generally follow the same approach. An organisation should consider its online service to be processing children's data when the service is intended for, or likely to be accessed or used by, a child. This means that in addition to services designed for children, services which are designed for mixed audiences, or services which are designed for adults but are in reality used by children, would also be deemed to be services processing children's data.

In assessing whether a service is likely to be accessed by children, regulators will typically consider factors such as the service's user demographic, design features, content, marketing channels and cultural relevance, rather than relying solely on the organisation's stated intent.

Given the potential scope, organisations should approach the assessment of whether a service is processing children's data carefully. While a practical and 'common sense' assessment is encouraged by the UK Information Commissioner's Office ('ICO') in its Children's Code, if an organisation considers itself to not be processing children's data, the ICO or an EU regulator will expect a strong, defensible argument as to why this position was taken, and likely expect the organisation to demonstrate ways in which the service actively excludes children from accessing or using the service.

Best interests of the child

Drawn from Article 3 of the UN Convention on the Rights of the Child ('UNCRC'), the fundamental principle which should be at the forefront for any organisation processing children's personal data is the best interests of the child. This – a theme which can be seen throughout other principles of children's data protection - can encompass many different elements including child safety, supporting development, protecting freedoms, and recognising the role of parents and guardians. Article 3 of the UNCRC states that:

> *"In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration."*

The UNCRC is often referenced by the ICO and EU regulators regarding the processing of children's data. According to the Children's Code for example, the UNCRC should be used as the basis for an organisation's assessment into the best interests of the child, particularly when designing a service. To do so, an organisation must first understand the rights of children as per the UNCRC and identify which may be relevant to their service, for example, the right to life, survival and development (Article 6), the right to respect for the views of the child (Article 12), and the right to protection of privacy (Article 16). While certain of these rights appear to go beyond the strict application of data protection, it is important that an organisation considers data processing activities associated with a service against the rights in order to identify potential impacts. For example, a service often includes data sharing. This could impact the right to life, survival and development (Article 6) in that sharing data could potentially expose children to risk of physical or emotional harm. Another example of common data processing through a service is profiling. This could impact the right to protection from economic exploitation (Article 32) in that this right is at risk where services use profiling for targeted advertising. Once an organisation has identified the potential impacts on UNCRC rights, it must assess the extent of the impact on children's rights and implement measures to mitigate the risks where relevant.

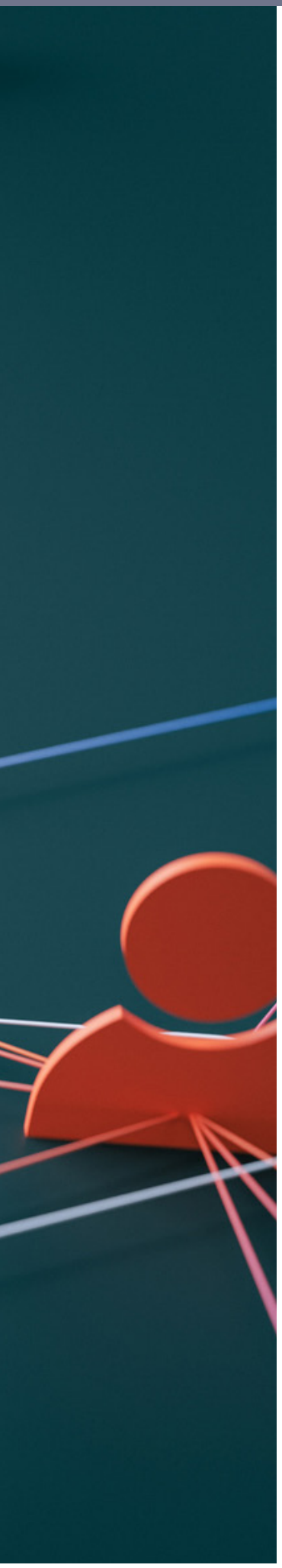
The process of assessing best interests should be a key priority for any organisation designing a new service or adding a new feature to a service aimed at, or likely to be used by, children

The process of assessing best interests should be a key priority for any organisation designing a new service or adding a new feature to a service aimed at, or likely to be used by, children. This should be approached as a specific form of privacy by design and default, a core principle which organisations are already familiar with. In practice, this requires organisations to be able to demonstrate how the best interests of the child were identified, assessed, and weighed against other considerations, particularly where product functionality, data monetisation, or user engagement objectives are involved. As stated by the ICO in the Children's Code, it is important to note that considering the best interests of the child does not mean a that an organisation cannot have commercial interests. However, where there is a conflict between commercial interests and a child's best interests, the latter should prevail.

Age appropriate application and verification

When complying with data protection requirements relating to children, it is important that an organisation operates 'age appropriate application', which means that the age range of users and the different needs and development of such age ranges are taken into consideration when designing and operating the service (i.e. age appropriate design is undertaken). A key regulatory expectation in this area is proportionality, and the level of age assurance adopted should reflect the nature of the service and the risks it presents to children. Like the best interests of the child, this principle should be woven through a children's data protection compliance programme, as it will touch on many areas, some of which are detailed below. For example, when complying with transparency requirements, the level of understanding of a child aged 6 will differ from a child aged 16, and an organisation should consider how best to meet the needs of both ages if using the same service.

In addition to being beneficial for child users, age appropriate application can also be beneficial for organisations. If an organisation has a mixed audience user base and does not operate age appropriate application, it is required to set the same standard of data protection for all users, meaning that it would be required to set the same standards for adults as children. This would



likely result in overly restrictive use of adult data, for example, certain settings defaulting to 'off' for all users, whereas for adults they would typically default to 'on'.

Age appropriate application is predicated on an organisation establishing the age range(s) of its users. Regulators use different terms when discussing this topic, namely 'age verification' and 'age assurance'. The common difference is that some regulators prefer to use the former as meaning there is a high degree of certainty in the age of the child, while the latter is more of an estimation as to the age of the child. Other regulators use 'age assurance' for the full spectrum of certainty. Notwithstanding the terminology, regulators agree that the methods which can be used for establishing the ages of users are non-exhaustive. Examples of measures include self-declaration, third-party verification services (usually based on attributes), and hard identifiers (e.g., a passport). Which measure or set of measures is appropriate for a service will depend on the nature of the service itself. Specifically, a service which would expose a child to a higher degree of risk should use a measure which results in a higher degree of certainty. When choosing the appropriate measure(s), the organisation should take into consideration whether the approach would result in further collection and processing of personal data and if so, whether this is reasonable and proportionate in the circumstances. For example, for a game aimed at children with minimal data processing, it would not be appropriate to collect passport information.

In addition to using these measures to understand the age of users, they should also be used to prevent children who are too young from accessing the service. If an online service is not intended for children (for example, a gambling website), measures appropriate to the level of risk should be implemented to restrict access.

Transparency

The GDPR requires transparency with respect to personal data and data processing activities, meaning that an organisation must be clear and open to users about how it processes their personal data. This obligation applies equally to children, with Article 12 of the GDPR stating that when providing information required under the GDPR, the information must be "in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child". Most organisations comply with transparency obligations by providing a privacy notice. From a regulatory perspective, transparency is assessed by reference to whether children are likely to understand how their data are being used, rather than whether information has merely been provided in a technically compliant format. Being transparent with children can require different methods of transparency, depending on the nature of the service and the age ranges of children. In most instances, a layered approach to transparency will be appropriate, with a privacy notice relevant to children operating as the foundation for transparency. This can be based on the 'adult' privacy notice, but should be amended to use language which children will understand. This often means using more casual or colloquial language, and removing information deemed excessive in the context. This can also include using diagrams, cartoons or other visuals. How an organisation may build up layers of transparency will depend on the nature of the service, but may include, for example, bite size or just-in-time notices which alert children to when data are being collected or processed in the context of a specific part of a service; video or audio descriptions of information which may be more digestible than written information; and interactive methods of delivering the information which are more likely to interest children over written information. Importantly, when the service is used by several age ranges of children, an organisation may need to consider preparing different age appropriate transparency measures.

For an organisation to achieve transparency effectively, involving children as stakeholders in the design process is an invaluable exercise. In its Fundamentals for a Child-Orientated Approach to Data Processing, the Irish Data Protection Commission includes extracts from children regarding views on transparency measures, demonstrating the effectiveness of engaging with children of different ages.

Data subject rights

For the purposes of the GDPR, a child is a data subject and is therefore entitled to benefit from the rights afforded to data subjects by law. The GDPR does not define an age which a child must be in order to exercise a data subject right, but there will be instances where it is more appropriate for an adult to exercise a data subject right on behalf of a child. Therefore, the general approach that organisations should take to data subject rights is that a child can exercise their own data subject rights at any time, as long as they have capacity to do so and it is in their best interests. If relevant following an assessment, the organisation should involve the parent or guardian in exercising the right. In performing this assessment, there are certain

factors which an organisation can take into consideration. For example, the age and maturity of the child (which may be demonstrated by interactions with the child), the context of the processing and the type of service (e.g. whether it is a higher risk activity such as related to a child's health), and whether complying with the right would be in their best interests (e.g. whether the child fully understands the consequences of complying with the right). To support consistent decision-making, organisations should consider implementing internal procedures to guide assessments of capacity and best interests, including escalation routes where it is unclear whether a child should exercise rights independently or with parental involvement.

How to approach compliance

When considering how to approach compliance with data protection requirements related to children, many organisations take the view of needing a specific programme operating within the larger data protection compliance programme. This is particularly true for organisations with mixed audiences and/or multiple services, as it allows the organisation to leverage elements of the existing programme for children's data. Common steps to take are:

- reviewing the business and services to understand where the touchpoints with children and children's data are or might be. As detailed above, it is important to approach this analysis with caution: a regulator will expect sufficient justification if an organisation considers children's data are not being processed;
- performing a best interests of the child analysis of the service. This should be the starting point before looking into more targeted measures; and
- once the organisation has determined what steps it needs to take, beginning to prepare measures to comply with the requirements.

While not covered in this article, other areas which may be relevant include default settings, parental controls, and data sharing. Where relevant, it will be greatly beneficial to the organisation to involve children as stakeholders in the preparation process.

Finally, while not the focus of this article, the protection of children online extends exponentially more broadly than data protection (for example, into online harms). As regulatory expectations continue to evolve, effective compliance with children's data protection requirements should be viewed as an ongoing, cross-functional exercise, closely aligned with broader online safety, product governance, and risk management frameworks. It is therefore important for organisations navigating compliance with children's data protection requirements to also be aware of other laws which may apply to children using their services.

Jonathan Wright | wrightj@hunton.com
Ashley Webber | awebber@hunton.com
Hunton