info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

PROTECTION OF CHILDREN IN DATA PROTECTION LAW
A Comparative Analysis of the EU GDPR and the UK GDPR

1. Introduction

The accelerating development of the digital age places minors in a particularly vulnerable position, as they come into contact with online platforms, social media, and digital services handling their personal data at an increasingly young age. The protection of children's data is therefore one of the most important and complex areas of modern data protection law, encompassing fundamental human rights, parental responsibility, corporate obligations, and the duties of state regulatory authorities.

The European Union's General Data Protection Regulation (GDPR)[1] established a unified data protection framework across EU Member States. Following its withdrawal from the European Union, the United Kingdom created an independent data protection regime: the UK GDPR[2], complemented by the Data Protection Act 2018[3], largely adopted the structure of the EU regulation, but differs from it in several respects, particularly in provisions concerning the protection of children.

The aim of this article is to comprehensively present and compare the rules relating to children under the EU GDPR and the UK GDPR, as well as the relevant secondary legal sources, regulatory guidelines, and the most significant differences between the two legal systems. The analysis covers age thresholds, mechanisms of parental consent, requirements for child-friendly data processing, specific rules applicable to online platforms, and issues of enforcement and sanctions.

2. The EU GDPR's rules regarding children

2.1. The age threshold and the issue of consent

Pursuant to Article 8 of the EU GDPR[1], in relation to information society services directly offered to a child, processing is lawful if the child is at least 16 years old. Member States may derogate from this, but the minimum permitted age is 13. This flexible regulation has resulted in significant differences within the EU: Hungary, the Czech Republic, Austria, and several other Member States have retained the age limit of 16, while Ireland and the United Kingdom (during its EU membership) set the threshold at 13, and France and Italy chose 15 and 14 respectively.

The implementation at Member State level is governed by the domestic laws of EU countries. In the case of Hungary, Act CXII of 2011 on informational self-determination and freedom of information[4] and Act XXXVIII of 2018[5] (the GDPR implementation act) contain relevant

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

provisions. In Hungary, the age of consent is 16, below which parental or legal guardian consent is required.

2.2. The obligation to verify parental consent

Article 8(2) of the GDPR[1] provides that the controller shall make reasonable efforts to verify that consent is given or authorised by the holder of parental responsibility, taking into consideration available technology. This "reasonable efforts" standard is relatively flexible and poses significant practical challenges, as in the online environment it is difficult to reliably verify the age of the user without engaging in disproportionate data collection.

The European Data Protection Board (EDPB) has issued several guidelines on this topic. The Article 29 Working Party Guidelines on consent under Regulation 2016/679.[6] address the interpretation of the age of consent under Article 8 and parental consent, discussing methods of age verification, including self-declaration, document-based, and technical solutions. The EDPB emphasises that age verification mechanisms must be proportionate to the risks associated with the processing.

2.3. Principles of data processing and special protection of children

The principles set out in Article 5 of the GDPR[1] in particular the principles of transparency, purpose limitation, data minimisation, and integrity are of heightened importance in the processing of children's data. Recital 38 of the GDPR[1] explicitly states that children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences, and safeguards concerned, as well as their rights in relation to the processing of personal data.
When applying the legal bases under Article 6 of the GDPR[1], particular attention should be paid to the applicability of legitimate interests (Article 6(1)(f)), where, in the case of children, increased care must be taken when carrying out the balancing test.

2.4. Data Protection Impact Assessment (DPIA) and Data Protection by Design

Carrying out a data protection impact assessment pursuant to Article 35 of the GDPR[1] is mandatory where the processing is likely to result in a high risk to the rights and freedoms of natural persons. The EDPB WP248 guidelines (a former Article 29 Working Party working document) specify when and how a data protection impact assessment (DPIA) must be conducted under the GDPR.
The application of the principles of privacy by design and privacy by default under Article 25 of the GDPR[1], in the case of children, means that services must be designed with the highest

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

level of data protection by default, and the principles of child-friendly design must be implemented already at the development stage.

3. The UK GDPR and related UK regulations

3.1. The General Framework of the UK GDPR and the DPA 2018

As a result of Brexit, the United Kingdom has had an independent data protection regime since 1 January 2021. The UK GDPR[2] is largely identical in substance to the EU GDPR; however, it contains a number of modifications reflecting the specificities of the United Kingdom. The Data Protection Act 2018 (DPA 2018)[3] complements the UK GDPR and, inter alia, includes specific provisions relating to children.
Article 8 of the UK GDPR sets the age threshold for consent at 13, in contrast to the default age limit of 16 under the EU GDPR. This difference is one of the most notable divergences between the two regimes and has practical implications for the provision of international digital services.

3.2. Az Age Appropriate Design Code (Children's Code)[7]

The most significant and innovative element of the UK regulatory framework is the Children's Code, formally titled *Age Appropriate Design: A Code of Practice for Online Services*. This code was issued by the Information Commissioner's Office (ICO).
The Children's Code sets out 15 standards that apply to online services directed at, or likely to be accessed by, children. Its scope covers websites, applications, social media platforms, online games, and any digital service that is likely to be used by individuals under the age of 18.

Key Requirements:

- Processing must, by default, serve the best interests of the child "Nudge techniques" that encourage children to weaken their protection or provide more data are prohibited. Data collection must be minimal (data minimisation)
- Geolocation must be switched off by default; profiling is only permitted where there is a justified reason and appropriate safeguards are in place
- Children's personal data may only be shared with third parties for marketing purposes in a strictly limited manner
- It is mandatory to formulate the Privacy Notice in child-friendly, clear, and understandable language
- Notification and messaging systems must not be used to encourage harmful use or to manipulate children into engagement

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

The impact of the Children's Code is already being felt beyond the United Kingdom: several major technology companies (including Instagram, TikTok, YouTube, and Google) have globally modified their data protection practices in order to comply with the requirements of the Code.

3.3. A Data (Use and Access) Act 2025[8]

The most recent data protection reform in the United Kingdom is set out in the Data (Use and Access) Act 2025, which amends but does not replace the UK GDPR and the Data Protection Act 2018.
The aim of the Act is to simplify data protection rules and promote innovation, while maintaining a high level of data protection safeguards.
The reform continues to treat the protection of children's data as a priority area and reinforces the application of the principle of "privacy by design and by default." In addition, a review of the Children's Code (Age Appropriate Design Code) is ongoing in order to align it with the new regulatory environment.

3.4. Relevant provisions of the Online Safety Act 2023[9]

From the perspective of children's online protection, data protection law is closely linked to the Online Safety Act 2023 (OSA 2023), which extends Ofcom's powers to supervise online service providers. The Act contains specific provisions for the protection of children and requires service providers to assess the risks of harmful content accessible to children (children's risk assessments) and to manage those risks.
Although the OSA 2023 is not a data protection law, it is closely connected to the UK GDPR and the Children's Code, as together they form a comprehensive regulatory framework for the protection of children online.

4. A Comparison of the EU GDPR and the UK GDPR: Key Differences and Similarities

4.1. Age threshold

One of the most significant differences lies in the determination of the age threshold for consent:

- **EU GDPR:** 16 years of age by default, with variations among member states ranging from 13 to 16 years
- **UK GDPR:** uniformly 13 years

This difference is particularly relevant for the 13–15 age group: in most EU Member States (including Hungary), parental consent is required, whereas in the United Kingdom this age

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

group can independently consent to the processing of their data. This divergence creates significant compliance challenges for digital services operating in both markets.

4.2. Special codes pertaining to children

While the EU GDPR does not contain a comprehensive and legally binding code on children's online protection comparable to the UK Children's Code, several EU Member States have developed national-level guidelines. At the EU level, the EDPB guidelines fulfil a similar role; however, by their nature, they are less detailed and specific than the UK Children's Code.
Within the EU, the Digital Services Act (DSA)[10], Regulation (EU) 2022/2065, contains specific provisions for the protection of minors. Large online platforms are required to carry out systemic risk assessments, including with regard to the protection of minors (Article 34). In addition, the Regulation prohibits targeted advertising based on personal data where the service provider is aware that the user is a minor Article 28(2).

4.3. Approaches to age verification

The EU and the UK hold differing positions on age verification:

- EU approach: The GDPR requires "reasonable efforts" (Article 8(2)[1] but does not prescribe specific technical solutions. The EDPB guidelines provide recommendations, but there is no binding technical standard.
- UK approach: The Children's Code sets more concrete expectations regarding the design of online services, and the ICO actively monitors compliance. In parallel, the Online Safety Act 2023 imposes broader obligations on platforms to protect children. It requires them to prevent minors from accessing certain harmful content, which in practice necessitates the use of effective age verification or age estimation solutions.

4.4. Profiling and automated decision-making

Both the EU GDPR and the UK GDPR prohibit decisions based solely on automated decision-making (including profiling) where such decisions produce significant effects on the data subject. This is particularly important in the case of children: Recital 71 of the EU GDPR explicitly states that special attention must be given to automated decision-making involving minors. The UK Children's Code requires that profiling-based features be switched off by default, unless the use of profiling can be justified by a compelling reason and serves the best interests of the child.

4.5. Penalties for Violations

Both systems impose strict penalties for violations:

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

- EU GDPR (Article 83): for the most serious infringements, up to 4% of the annual global turnover or €20 million, whichever is higher.
- UK GDPR / DPA 2018: the ICO may impose fines of up to £17.5 million or 4% of the annual global turnover.
- Online Safety Act 2023: the Act grants Ofcom extensive fining powers, which, according to official government guidance, may reach up to 10% of a company's global annual revenue

In the application of the sanctioning system, both authorities, the member authorities of the EDPB and the ICO, consider infringements affecting children to be particularly serious, and treat the involvement of minors as an aggravating factor when determining the amount of fines.

5. Special Areas and Challenges

5.1. Social Media and Influencer Marketing

Social media platforms are particularly affected by regulations on children's data protection. In recent years, significant regulatory proceedings have been initiated against Instagram, TikTok, and YouTube both in the EU and in the United Kingdom, in several cases resulting in substantial fines.

In the field of influencer marketing, relevant consumer protection rules in the European Union are set out in Directive 2005/29/EC on unfair commercial practices (UCPD), as amended by Directive (EU) 2019/2161 (Omnibus Directive)[11]. These establish a general prohibition of misleading and aggressive commercial practices, which in practice must also be applied to influencer marketing, particularly to communications directed at children.

In the United Kingdom, advertising is supervised by the Advertising Standards Authority (ASA), which, under the CAP Code, prohibits advertising practices that are harmful or misleading to minors, including certain forms of influencer marketing.

5.2. **Online games**

Online games present particular challenges, as children are highly active in these environments and gaming platforms collect vast amounts of data about them. Under both the GDPR and the UK GDPR, loot boxes, targeted advertising, and the encouragement of in-game purchases all raise data protection and consumer protection concerns. Both the EDPB and the ICO's Children's Code provide guidance on how the use of gamification elements affects children's data protection.

5.3. Educational Technology (EdTech) and School Data Management

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

In the field of educational technology, the processing of children's data in schools is a particularly sensitive issue. In the European Union, the legal basis for data processing for educational purposes is typically provided by Article 6(1)(c) (legal obligation) or (e) (performance of a task carried out in the public interest) of the GDPR, especially in the case of public educational institutions.
In the United Kingdom, such processing is governed jointly by the Data Protection Act 2018 and the UK GDPR, while Schedule 1 of the DPA 2018 primarily sets out the conditions for processing special categories of data. Recital 91 of the GDPR emphasises that, in the case of processing by public authorities, conducting a data protection impact assessment (DPIA) may be particularly justified, which is also applicable to data processing in schools.

5.4. Artificial Intelligence and Children

The EU AI Act (Regulation (EU) 2024/1689)[12] is of particular importance in the regulation of artificial intelligence systems affecting children. Although the Regulation does not establish a separate, comprehensive regime specifically dedicated to children, they receive special attention as a vulnerable group of users. Among high-risk AI systems (Annex III) are, inter alia, systems used in education and those applied for the evaluation of natural persons and decision-making, which often affect minors. The combined application of the AI Act and the GDPR therefore results in complex compliance obligations in the case of AI systems involving children.
In the United Kingdom, the regulation of artificial intelligence primarily follows a principles-based approach, in which the Information Commissioner's Office (ICO) provides detailed guidance on the application of data protection requirements through its "AI and Data Protection Guidance" document.

6. Enforcement of Rights and Administrative Practice

6.1. EU regulatory procedures

In the EU, under the one-stop-shop mechanism, the lead supervisory authority coordinates the supervision of cross-border data processing. The Irish Data Protection Commission (DPC), acting as the lead authority for many technology giants in Europe, has investigated numerous cases concerning children's data protection:

- Meta (Instagram): €405 million fine – default public settings for children's profiles
- TikTok: several EU Member State authorities have conducted investigations regarding the processing of children's data
- YouTube/Google: multiple Member States have initiated investigations concerning behavioural targeted advertising directed at children

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

The EDPB's coordinating role is crucial: the binding decision-making procedures under Article 65 and the EDPB's strategic priorities place a high priority on the protection of children's data.

6.2. The ICO's regulatory activities in the UK

The ICO pursues an active enforcement policy in the area of children's data protection.

Note:

- TikTok: £12.7 million fine (2023) – unlawful processing of personal data of children under the age of 13 in violation of the UK GDPR
- As part of the enforcement of the Children's Code, the ICO has carried out audits and investigations affecting several online service providers, including social media, gaming, and edtech platforms

The ICO also conducts regular compliance checks and publishes detailed guidance on the protection of children's data

Its enforcement activities, based on the ICO Children's Code, serve as a model for EU member states and influence the development of the EDPB's guidelines.

7. Summary and Conclusions

A comparison of the provisions of the EU GDPR and the UK GDPR concerning children offers a number of important lessons for legislation, law enforcement, and corporate compliance.

7.1. Summary table of the main differences

Age of consent

- EU GDPR: 16 years (with Member State variation between 13–16)
- UK GDPR: uniformly 13 years

Child-specific code:

- EU GDPR: no unified binding code (EDPB guidelines)
- UK: Children's Code

Online safety legislation:

- EU: Digital Services Act (2023)
- UK: Online Safety Act (2023)

AI regulation:

- EU: AI Act (2024)

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

- UK: AI Opportunities Action Plan

The maximum amount of the fine:

- In the European Union, under the GDPR, the maximum fine for the most serious infringements is €20 million or 4% of the undertaking's total worldwide annual turnover, whichever is higher.
- In the United Kingdom, the UK GDPR and the Data Protection Act 2018 apply a similar sanctioning system, under which the ICO may impose fines of up to £17.5 million or 4% of global annual turnover.
- By contrast, the Online Safety Act 2023 grants Ofcom broader fining powers, which, according to official government and regulatory communications, may reach up to 10% of a company's global annual turnover

7.2. Similarities and Differences

Despite the fact that the EU GDPR and the UK GDPR originate from common foundations, a clear divergence can be observed in the area of children's protection: the United Kingdom, through the Children's Code and the Online Safety Act, has developed a stronger, more specific, and more detailed regulatory regime, whereas the EU has formulated more general principles, which are complemented by the DSA and the AI Act.

At the same time, a common feature of both systems is that they treat the protection of children's data as a priority, provide for severe sanctions in cases of infringement, and see authorities actively enforcing the rules against major technology platforms. The two systems mutually influence each other: the UK Children's Code has inspired similar initiatives in several EU Member States, while EDPB guidelines continue to evolve in light of UK practice.

7.3. Future Outlook

Both EU and UK data protection law are evolving dynamically in the area of children's protection. At the EU level, developments are expected in the implementation of the DSA and the AI Act, the issuance of new EDPB guidelines, and the refinement of Member State-level implementation. In the UK, changes may arise from the entry into force of the DUAA (Data (Use and Access) Act 2025) and the enforcement of the OSA 2023 by Ofcom. The emergence of artificial intelligence and next-generation digital services will create further challenges, to which both legal systems will need to respond flexibly.
The protection of children's data is one of the areas where the development of law and technology is the most rapid, and where authorities are the most active therefore, for organisations operating in this field, continuous compliance and proactive child-friendly design are fundamental expectations.

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

Legal References and Bibliography

1. Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR).
2. UK General Data Protection Regulation (UK GDPR)
3. Data Protection Act 2018 (DPA 2018)
4. Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (Hungary).
5. Act XXXVIII of 2018 on the implementation of data processing provisions defined in the General Data Protection Regulation of the European Union (Hungary).
6. Article 29 Working Party Guidelines on consent under Regulation 2016/679.
7. Age Appropriate Design Code (Children's Code).
8. Data (Use and Access) Act 2025.
9. Online Safety Act 2023 (OSA 2023).
10. Regulation (EU) 2022/2065 of the European Parliament and of the Council (19 October 2022) on a Single Market for Digital Services (Digital Services Act – DSA).
11. Directive (EU) 2019/2161 of the European Parliament and of the Council (Omnibus Directive) – on better enforcement and modernisation of Union consumer protection rules, in particular amending Directive 2005/29/EC.
12. Regulation (EU) 2024/1689 of the European Parliament and of the Council (13 June 2024) laying down harmonised rules on artificial intelligence (EU AI Act).