A comparison of key children's privacy requirements in the UK, Germany, France and U.S., September 2023

	United States	United Kingdom	Germany	France
Relevant legislation	Children's Online Privacy Protection Act 1998 (COPPA)	• Age Appropriate Design Code (AADC) • General Data Protection Regulation (UK GDPR)	• Interstate Treaty on the Protection of Minors in the Media (Jugendmedienschutz-Staatsvertrag – JMStV) • Federal Youth Protection Act (Jugendschutzgesetz – JuSchG) • Interstate Media Treaty (Medienstaatsvertrag – MStV) • Telecommunication-Telemedia Data Protection Act (Telekommunikation-Telemedien-Datenschutz-Gesetz – TTDSG). • General Data Protection Regulation (GDPR) Note that the EU's Digital Services Act (DSA) also contains rules for online platforms to ensure a high level of privacy for minors (U18s) – but the requirements are not addressed in this table.	• Law on digital majority and the fight against online hate (DMFAOH law) • French Data Protection Act (FDPA) • General Data Protection Regulation (GDPR) • CNIL's (French data protection agency) eight recommendations to enhance the protection of children online (Recommendations) • Decree implementing Law no. 2022-300 (Decree) Note that the EU's Digital Services Act (DSA) also contains rules for online platforms to ensure a high level of privacy for minors (U18s) – but the requirements are not addressed in this table.
What is the age of a child in the legislation?	Under the age of 13.	Under the age of 18. However, the AADC also requires companies to think about what is appropriate depending on the age of the child – for example, a five-year-old will need protecting differently from a 16-year-old and will be less capable of understanding choices and data usage. It provides some suggested different age band recommendations, but these are not mandatory.	Under the age of 18. The JMStV and JuSchG distinguish between: • Children (under the age of 14); and • Adolescents (aged 15 to 17). Aside from the above, the legal age of majority in Germany, i.e. the age at which individuals are able to enter into legally binding contracts without any legal limitations (such as parental approval), is 18.	Under the age of 15. However, the law distinguishes the data processing of minors according to their age: • A minor **under 13** is unable to consent to personal data processing. • For minors aged **between 13 and 15**, consent to process personal data must be obtained from the minor **and** from a holder of parental authority. • Minors **over 15** may give consent to the processing of personal data. Aside from the above, the legal age of majority in France, i.e., the age at which individuals are able to enter into legally binding contracts without any legal limitations (such as parental approval), is 18.
What services does it apply to?	Websites, mobile applications, IOT or connected products or other online services or platforms that are "directed to children." Whether a site or service is "directed to children" depends on a number of factors, including: • The subject matter of the site or service. • Visual and audio content. • The use of animated characters or other child-oriented activities and incentives. • The ages of models. • The presence of child celebrities or celebrities who appeal to children, ads on the site or service that are directed to children, and other reliable evidence about the age of the actual or intended audience.	Online services that are "likely to be accessed by" children, which means that the possibility of children accessing the service needs to be "more probable than not."	The JMStV applies to broadcasting (i.e., linear services) and digital services (i.e., websites and online services, including audiovisual services). The JMStV does not apply to content distributed on carrier media (such as DVDs). The JuSchG applies to digital services and content distributed on carrier media (such as DVDs).	Online services (including online social networking services) and data processing based on the user's non-contractual consent.

A comparison of key children's privacy requirements in the UK, Germany, France and U.S., September 2023

	United States	United Kingdom	Germany	France
What are the requirements on age gating?	A website or online service directed to children must treat all visitors as children and provide COPPA's protections to every such visitor, meaning that the website or service may not screen users for age. However, if the website or service does not target children and is not intended for children as its primary audience but is deemed to be "directed to children" based on an examination of factors (see above), then an age gate is permitted to screen for users who indicate they are children under 13 and therefore to ensure that the website or service does not collect personal information from those users or else obtains "verifiable parental consent." If the website or online service is directed to children, but not primarily so, it can implement this age gate so long as (i) it does not collect personal information from any visitor prior to collecting age information, including through the use of cookies; and (ii) it prevents the collection, use or disclosure of personal information from visitors who identify themselves as under the age of 13 without first complying with the "verifiable parental consent" requirements (see below). A website or online service that is not deemed to be directed to children does not need to have an age gate.	A website or online service that is "likely to be accessed by" children should treat all visitors as children and apply the AADC requirements to any data processing (for which, see below) unless it can separate out adult and child users. Therefore, there is no requirement to age gate, but age gating is one option to ensure that only adults use the services or to separate out child users to whom the AADC requirements apply and thereby avoid the restrictions in the AADC otherwise being applied to all users.	**Age gating.** Providers transmitting or making available content that might risk impairing the development of children or adolescents of certain age groups must ensure that children or adolescents falling within the respective age group are in general unable to view or listen to such content. The law distinguishes between the following age groups: (i) six to eleven years old, (ii) 12 to 15 years old, (iii) 16 to 17 years old, and (iv) 18 years and older. A provider may fulfill this obligation by: • Making it impossible, or very difficult, for children within the respective age group to gain access to or awareness of the content, by using technical or other measures, or by assigning an age rating to the content that can be read by appropriate, certified software systems used to restrict access by minors for their protection; or • Limiting the hours during which the content is accessible in a manner that ensures that children or adolescents within the respective age group are in general unable to view or listen to such content. **Precautionary measures.** Certain providers that store or make available third-party information and that offer services to children and adolescents must implement appropriate and effective structural precautionary measures to ensure their protection, such as providing a reporting and redress mechanism, providing an age verification tool, or having in place specific default settings. **Age rating.** There is a general requirement to rate content. This is a precondition for compliance with the obligation to have age gates in place. **Media considered as harmful to minors** cannot be classified (i.e., a rating is refused). **Rating bodies.** In line with the German approach of "regulated self-regulation," there are a number of accredited rating bodies. Although there is no requirement to join such a rating body, membership ensures that the German Federal Commission for Youth Media Protection (Kommission für Jugendmedienschutz – KJM) will first engage the relevant rating body in the clearance process before enforcing the provisions of the JMStV against the provider. **Video-sharing platform providers**, who do not have editorial responsibility for the content made available, are required to: • Take appropriate measures to protect minors from content that may impair the physical, mental or moral development of children and adolescents, such as age verification tools or tools that enable parents to restrict and monitor access to such content; and • Implement systems that enable users to rate content that they upload to the video-sharing platform. **Providers of movie and games platforms** may only offer content that has been age rated and labeled accordingly. The GDPR provides that consent controls must consider the technological means that are available.	The GDPR provides that consent controls must consider the technological means that are available. The DMFAOH law provides that to verify the age of end-users (and obtain authorization from one of the holders of parental authority), social network service providers must use technical solutions that comply with a set of guidelines drawn up by the Audiovisual and Digital Communication Regulatory Authority (ARCOM), following consultation with the CNIL. (The DMFAOH law will enter into force at a later date, not yet determined. Sanctions for noncompliance will be enforced one year after its enactment, while parental authorization for existing networking accounts will come into effect two years after its enactment.) The Recommendations restate the requirements for "verifying a child's age and parental consent while respecting the child's privacy," in particular to comply with the obligations of the GDPR and the law on minors' access to social networks. Age verification systems should be structured around six principles: • Minimization • Proportionality • Robustness • Simplicity • Standardization • Third-party intervention The Decree mandates the installation of parental control mechanisms on terminals placed on the French market. This includes parents being able to block app store content legally prohibited to those under 18.

A comparison of key children's privacy requirements in the UK, Germany, France and U.S., September 2023

	United States	United Kingdom	Germany	France
What consent is needed from the parent?	Operators of a website or online service directed to children must obtain "verifiable parental consent" for the collection, use or disclosure of children's personal information. There are several methods to obtain verifiable parental consent, and the appropriateness of the method depends on whether the operator will disclose children's personal information to third parties, or allow children to make it publicly available, in which case the standard for adequate consent is higher. To obtain the highest degree of flexibility with regard to a child's personal information, the operator could require the parent to: • Provide a signed consent form; • In connection with a monetary transaction, use a credit card, debit card or other online payment system that provides notification of each discrete transaction to the primary account holder; • Call a toll-free telephone number; • Participate in a video conference; • Provide a form of government-issued identification to be compared against databases of such information; • Answer a series of knowledge-based challenge questions; or • Submit a picture of a driver's license of other photo ID to be compared using facial recognition technology against a separate photo submitted by the parent. If the operator is only going to use children's personal information for internal purposes (i.e., no disclosure to third parties and no ability for the child to disclose it to others), then it is also possible to use an "email plus" method of parental consent, which enables the parent to consent in a return email after receipt of direct notice about the operator's privacy practices. Note: There are some exceptions in specific situations.	The AADC isn't focused on getting consent from an adult for processing their child's personal data in the same way as COPPA. Instead, it is essentially about doing less data processing for children who use services and protecting their data more stringently regardless of what the adult says. It would not therefore be possible to simply override the AADC requirements by getting a parent to give or waive consent. Outside of the AADC, consent from a parent is needed where the UK GDPR requires it for online services such as when relying on consent for processing data – for example, for direct marketing or for the installation of cookies – and the child is under the age of 13.	The JMStV is not focused on getting consent from the adult for processing their child's personal data in the same way as COPPA. Consent from a parent is needed where the GDPR requires it for online services such as when relying on consent for processing data – for example, for direct marketing or for the installation of cookies – and the child is under the age of 16.	Under the GDPR, the controller must make reasonable efforts to verify that consent is given by a holder of the parental authority. Consent must be: • Given Freely; • Specific; • Informed; and • Unambiguous. The DMFAOH law provides that online social networking service providers must obtain the express authorization of one of the holders of parental authority for: • New accounts created by minors aged 13 to 15; and • Accounts already created and held by minors aged 13 to 15. New accounts for minors aged 16 or 17 do not require parental consent. Consent from only one holder of parental authority is enough.
What data does it apply to?	There is a specific list of items of data caught by the legislation. Although the list is enumerated, and therefore defined, it also includes persistent identifiers, and items that could be construed broadly, including "information concerning the child or the parents of that child that the operator collects online from the child and combines with" any of the specifically enumerated items.	The AADC does not have a specific list but applies to all personal data (using the broad definition in the UK GDPR) including the "processing" of that personal data (again using the UK GDPR definition). However, some types of processing activities are seen as potentially harmful to and not in the best interests of the child and are therefore addressed through the restrictions (see below).	Neither the JMStV nor the JuSchG regulate the processing of the personal data of minors. Processing of the personal data of minors is subject to the more generic requirements of the GDPR and the Federal Data Protection Act, as well as the sector-specific requirements of the TTDSG.	The GDPR protects the use of children's personal data for marketing purposes or to create personality or user profiles. It also applies to the collection of personal data when children use services that are offered to them directly. The FDPA applies to all personal data.

A comparison of key children's privacy requirements in the UK, Germany, France and U.S., September 2023

	United States	United Kingdom	Germany	France
What are the information requirements?	Operators must provide both a privacy policy anywhere children's information is collected, and a direct notice to parents. Direct notices to parents of children must include various information including the types of personal information collected, that parental consent is required and how to provide consent. If the parent doesn't consent within a reasonable time, operators must delete the parent's online contact information from their records. There are strict notice requirements on the information that must be contained in a privacy policy for all operators that collect personal information, including details on the types of children's personal information collected and how it is used, and a description of parental rights.	Before a covered business rolls out a new feature or product, the business must complete a data protection impact assessment (DPIA). The DPIA must take into account differing ages, capacities, and developmental needs of children. The AADC focuses on making privacy information age appropriate. There are no new specific items of information that have to be given, but the AADC requires that privacy policies, privacy settings, and controls and prompts (which are already required under the UK GDPR) need to be designed to be understandable and child friendly. This might, for example, include adding in videos, cartoons, infographics, etc. It also requires organizations to provide additional "bite-sized" explanations about how they use personal data at the point that use is activated.	Depending on the nature of the services and the size of the company providing them, there may be a requirement to appoint a youth protection officer (Jugendschutzbeauftragter) and to make their contact details, including their name and electronic means of communication, easily and directly accessible. Providers of telemedia services the content of which is materially identical to movies or games on carrier media (which are subject to the age rating and labeling requirements under the JuSchG) must include information on such age ratings and labeling. Where personal data is processed, the GDPR information requirements apply.	The DMFAOH law provides that when a user aged 13 to 15 tries to register for an online account, companies must provide information to them and to those with parental authority on the risks associated with digital use and the means of prevention. They must also provide users under the age of 15 with clear and appropriate information on the conditions of use of their data and rights guaranteed by the FDPA. To this end, the minor must be informed of: • The purposes for which their personal data is being collected, as well as the identity of the recipient(s) of that data; • The mandatory or optional nature of the fields the minor is asked to complete; • The right to access any personal data to verify its accuracy and, if necessary, have it rectified or deleted; and • The right to object to the collection and use of any personal data. Like the AADC, the Recommendations focus on enhancing children's access to information and their rights by design. This includes providing versions of terms and privacy policies that meet the age-appropriate information requirements (clear, simple and engaging). The Recommendations also recommend presenting information to children in a manner that speaks to them in their own language and captures their attention. This can mean, for example, using clear, simple and short sentences, and using interactive elements such as icons, videos or images. The Recommendations also aim to encourage parental involvement in their children's digital education. The Decree states that manufactures must provide an explanatory note that makes the exact functionalities offered by the device easily accessible and understandable.
What are the restrictions and obligations on data use?	The focus is on getting parental consent rather than new restrictions on what can be done with data. But the law provides some requirements as to how data can be used and accessed, including that operators who collect personal information subject to COPPA must: • Provide parents with a means of reviewing the personal information collected. • Take "reasonable" precautions before sharing information with third parties, including periodic monitoring, to confirm that any service providers or third parties with whom the operator shares children's personal information maintains the confidentiality and security of that information. • Retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected.	The AADC has 15 standards that must be met when processing children's personal data. These contain various requirements and restrictions, the key ones being: • Privacy settings must be set at "high privacy" by default. • Profiling (for example, for targeted advertising but also for personalization and anything that is beyond the "core service") should be switched off by default. • Nudge techniques can't be used – for example, encouraging a child to change the settings that protect their privacy. • Data should not be shared unless there is a compelling reason to do so. • Geolocation should be switched off by default. An obvious sign should be provided to children when location tracking is active. • Only data that is necessary should be processed. All processing should be in the "best interests of the child" (which must be a "primary consideration" when designing and developing the service). This means thinking about access to harmful content, considering children's mental health through pausing or not having the continuous scroll feature, evaluating the potential harm of "like" buttons, etc. • Data cannot be used in a way that is detrimental to children's wellbeing.	• Where a telemedia service provider processes the personal data of minors for the purpose of protecting minors, for example, through age verification measures or other technical measures, such personal data must not be processed for commercial purposes, such as direct marketing, profiling, and behaviorally targeted advertising. • If personal data is processed for journalistic purposes, such data must not be processed for other purposes.	The CNIL recommends deactivating by default any profiling systems for children, especially for the purposes of targeted advertising, and refraining from reusing children's data or sharing it with third parties for commercial or advertising purposes, unless the services can demonstrate that they are acting for compelling reasons in the best interests of the child. The Recommendations also require stricter default privacy settings. Privacy settings should be simple to change, and certain options such as geolocation should be disabled by default. Moreover, the DMFAOH law entitles a holder of parental authority to request online social networking service providers to suspend the account of a minor under the age of 15. The Decree states that the personal data of minors collected or generated during the activation of parental controls on the device must not be used for commercial purposes, such as direct marketing, profiling, and behavioral advertising.

A comparison of key children's privacy requirements in the UK, Germany, France and U.S., September 2023

	United States	United Kingdom	Germany	France
Enforcement and penalties	COPPA may be enforced concurrently by the Federal Trade Commission, or other federal agencies, and state attorneys general. Penalties of up to $46,517 per violation may be assessed.	The ICO has powers to impose administrative fines under the UK GDPR of up to £17.5 million or 4% of an organization's annual worldwide turnover, whichever is higher.	The JMStV is enforced by self-regulatory bodies and the state media authorities, the latter acting through the KJM. It is a criminal offence under the JMStV to distribute or make available content that is clearly capable of seriously jeopardizing the development or education of children or adolescents. It is a criminal offence under the JuSchG to distribute content that is considered harmful to children or adolescents, and to perform certain similar/related acts. Several JMStV violations constitute an administrative offence, including not having in place sufficient age gating. The processing of personal data of minors for commercial purposes, where this data was acquired for the purpose of protecting minors, constitutes an administrative offence under the TTDSG. Under the GDPR, fines of up to €20 million or 4% of an organization's annual worldwide turnover, whichever is higher.	The DMFAOH law is enforced by ARCOM. According to the law, when a social network service provider fails to implement a certified technical solution for the age verification of end-users and there is no authorization from a holder of parental authority for the registration of minors under the age of 15, the president of ARCOM will send the provider, by any means capable of establishing the date of receipt, a formal notice requiring the provider to take all measures necessary to meet these obligations. The provider has 15 days from the date of the formal notice to report back. At the end of this period, in the event of a failure to comply with the requirements of the formal notice, the chairman of the French Audiovisual and Digital Communications Regulatory Authority may refer the matter to the president of the Paris Court of First Instance, with a view to ordering the provider to implement a compliant technical solution. The penalty for failing to do so is a fine not exceeding 1% of the social network service providers worldwide sales for the previous financial year. The new obligations imposed in the Decree will be monitored by the National Frequency Agency, which may impose sanctions. Non-compliant terminals may also be prohibited from being placed on the market or removed from the market by ministerial order. Under the GDPR, fines of up to €20 million or 4% of an organization's annual worldwide turnover, whichever is higher.