ReedSmith

A comparison of key UK, German and US kids privacy requirements, 22 September 2022

Issue	California	United States	United Kingdom	Germany
Title	California Age Appropriate Design Code Act (**AADCA**)	Children's Online Privacy Protection Act 1998 (**COPPA**)	Age Appropriate Design Code (**AADC**)	Jugendmedienschutz-Staatsvertrag (**JMStV**)
What is the age of a child in the legislation?	Under the age of 18.	Under the age of 13.	Under the age of 18. However, AADC also requires companies to think about what is appropriate depending on the age of the child – for example, a 5 year old will need protecting differently to 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.	The German Interstate Treaty for the Protection of Minors in the Media (Jugendmedienschutz-Staatsvertrag – "JMStV") distinguishes between: • Children (under the age of 14); and • Adolescents (under the age of 18). Apart from the above, in Germany the legal age of majority, i.e. the age upon which persons are able to enter into legally binding contracts without any legal limitations (such as parental approval), is 18.
What services does it apply to?	Online services, products or features which are "likely to be accessed by" children, which means that it is reasonable to expect (based on certain indicators) that they would be accessed by children, including: • Being directed to children, as defined by COPPA • Being routinely accessed by a significant number of children, based on competent and reliable evidence on audience composition (or is substantially similar or the same as another online service, product or feature determined to be) • Having a significant child audience based on internal company research • Advertising to children • Having design elements known to be of interest to children, including games, cartoons, music and celebrities who appeal to children.	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" can depend 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 age of models, • the presence of child celebrities or celebrities who appeal to kids, 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 which are "likely to be accessed by" children, which means that the possibility of children accessing the service needs to be "more probable than not".	Broadcasting (i.e. linear services) and telemedia (i.e. websites and online services, including audiovisual services). The JMStV does not apply to content distributed on carrier media (such as DVDs). The content distributed on carrier media must comply with the provisions of the Federal Youth Protection Act (Jugendschutzgesetz – "**JuSchG**").

What are the requirements on age gating?	A website or online service that is likely to be accessed by children should either estimate the age of child users with a "reasonable level of certainty appropriate to the risks of the business' data management practices", or treat all users as child users by applying the privacy and data protections to everyone.	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 (1) it does not collect personal information from any visitor prior to collecting age information, including through the use of cookies; and (2) it prevents the collection, use, or disclosure of personal information from visitors who identify themselves as under age 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 similarly 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. There is no requirement to age gate therefore but age gating is one option for ensuring that only adults using the services or for separating out child users to apply the AADC requirements to and thereby avoid the restrictions in the AADC having to otherwise be applied to all users.	**Age gating.** Providers transmitting or making accessible content suited to impair the development of children or adolescents shall ensure that children or adolescents of the relevant age group (i.e., (i) 6 years or older, (ii) 12 years or older, (iii) 16 years or older, and (iv) 18 years or older) do not normally see or hear such content. A provider may fulfil this obligation by: • making access and perception of the content impossible or very difficult for children or adolescents of the respective age group via technical or other measures, or by fitting the content with an age rating which can be read by suitable technical systems for the protection of minors (i.e. certified computer software intended to restrict access by minors); or • limiting the day-time during which the content can be accessed in a manner that ensures that children or adolescents of the respective age group do not normally see or hear the content. **Age rating.** There is a general requirement to rate content. This is a pre-condition for compliance with the obligation to have age gates in place. **Media considered as harmful to minors** cannot be classified (rating refused). **Rating bodies.** Following the German approach of "regulated self-regulation", there is a number of accredited rating bodies. There is no requirement to join such rating body, however membership will result in the *German Federal Commission for Youth Media Protection (Kommission für Jugendmedienschutz* – "**KJM**") not enforcing the JMStV primarily against the provider, but first involving the relevant rating body for clearance. **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 which may impair their physical, mental or moral development of children and adolescents, such as age verification tools or tools that enable parents to restrict and control access to such content; • 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 labelled accordingly

What consent is needed from the parent?	The AADCA does not have a parental consent mechanism. Parental consent requirements under COPPA still apply when information is collected online from children U13.	Operators of a website or online service directed to children must obtain "verifiable parental consent" for the collection, use, or disclosure of personal information from children. 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 that which is 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; • Require in connection with a monetary transaction, use of 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; • Video conference; • Provide a form of government-issued identification to be compared against databases of such information; • Require a parent to answer a series of knowledge based challenge questions; or • Submit a picture of a driver's license of other photo ID submitted by the parent and then comparing that photo to a second photo submitted by the parent, using facial recognition technology. 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 for specific situations.	The AADC isn't focused on getting consent from the adult for processing their child's 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 agree/waive it. Outside of AADC, consent from a parent is needed where GDPR requires it for online services such as if 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 in the UK.	The JMStV is not focused on getting consent from the adult for processing their child's data in the same way. Consent from a parent is needed where GDPR requires it for online services such as if 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 in Germany.

What data does it apply to?	The AADCA does not apply to specific types of data, rather, it applies to online services, products or features likely to be accessed by children.	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.	AADC does not have a specific list but applies to all personal data (using the broad definition in GDPR) and it applies to "processing" of that personal data (again using the GDPR definition). Some types of processing activities are seen as potentially harmful to and not in the best interests of the child however and are therefore addressed through the restrictions (see below).	The JMStV does not regulate the processing of personal data (of minors). Processing of 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 Telecommunication-Telemedia-Data Protection Act ("**TTDSG**").
What are the information requirements?	Before a covered business rolls out a new feature or product, the business must complete a Data Protection Impact Assessment ("DPIA"). The DPIA should address whether the design of the product or feature is likely to expose children to harmful content, experience, be targeted or exploited by harmful contacts, witness or participate in harmful conduct, , whether targeted advertising or algorithms could harm children, whether automatic playing of media or features designed to increase time spent using the product could harm children, and whether any sensitive personal information is collected or processed. The DPIA should identify material risks to children and create a plan to remediate those risks. Businesses may be required to provide DPIA's to the California Attorney General. Covered businesses are also required to: • Provide terms of service and privacy notices in terms that are capable of being understood by children that are likely to access the service • Provide prominent notices and tools to help children exercise their privacy rights	Operators must provide both a privacy policy anywhere children's information is collected, and a direct notice to parents. Direct notice 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 your records. There are strict notice requirements on the information that must be contained in a privacy policy, all operators that are collecting personal information, the types of the child's personal information collected and how it is used, and a description of the parents' 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 the child. The AADC focuses on making privacy information age-appropriate. There are no new specific items of information that have to be given but AADC means that privacy policies and Privacy Settings and controls and prompts (already required under 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 organisations to provide additional "bite-sized" explanations about how you use personal data at the point that use is activated.	The JMStV does not regulate the processing of personal data (of minors). Depending on the nature of the services and the company size of the provider, there may be a requirement to appoint a youth protection officer (Jugendschutzbeauftragter) and to provide their contact details, including name and electronic means of communication, in an easily and directly accessible manner. 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 labelling requirements JuSchG) have to include information on such age ratings and labelling.
What are the restrictions and obligations on data use?	Websites and services likely to be accessed by children must: • Configure default privacy settings to offer a high level of privacy Websites and services likely to be accessed by children are prohibited from doing the following: • Using personal information in a way that could be materially detrimental to the child • Profiling children by default	The focus is on getting parental consent rather than new restrictions on what can be done with data. But the Rule provides some requirements as to how data can be used and accessed, including that operators who have collected 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 maintain the confidentiality and	AADC has 15 standards that must be met when processing children's 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 personalisation and anything which is beyond the 'core service') should be switched off by default. • Nudge techniques can't be used – for example that encourage a child to change settings which protect their privacy.	• Where a telemedia service provider has processed personal data of minors for the purpose of protecting minors, e.g. through age verification measures or other technical measures, such personal data must not be processed for commercial purposes, such as direct marketing, profiling and behaviourally targeted advertising. • If personal data is processed for journalistic purposes, such data must not be processed for other purposes.

	• Using dark patterns to induce a child to provide personal information beyond what is reasonably necessary • Collect geolocation information without providing a clear signal that the service is actively collecting such information • Collect any personal information beyond what is necessary to provide the product or service.	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.	• 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 which 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 their mental health through pause/not having continuous scroll, the potential harm of like buttons etc. • Data cannot be used in a way that is detrimental to children's wellbeing.	
Enforcement and Penalties	AADCA is enforced by the California Attorney General. There is no private right of action. Penalties range from: • $2500 for negligent violations per affected child; to • $7500 for intentional violations per affected child.	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 organisations annual worldwide turnover, whichever is higher.	

****