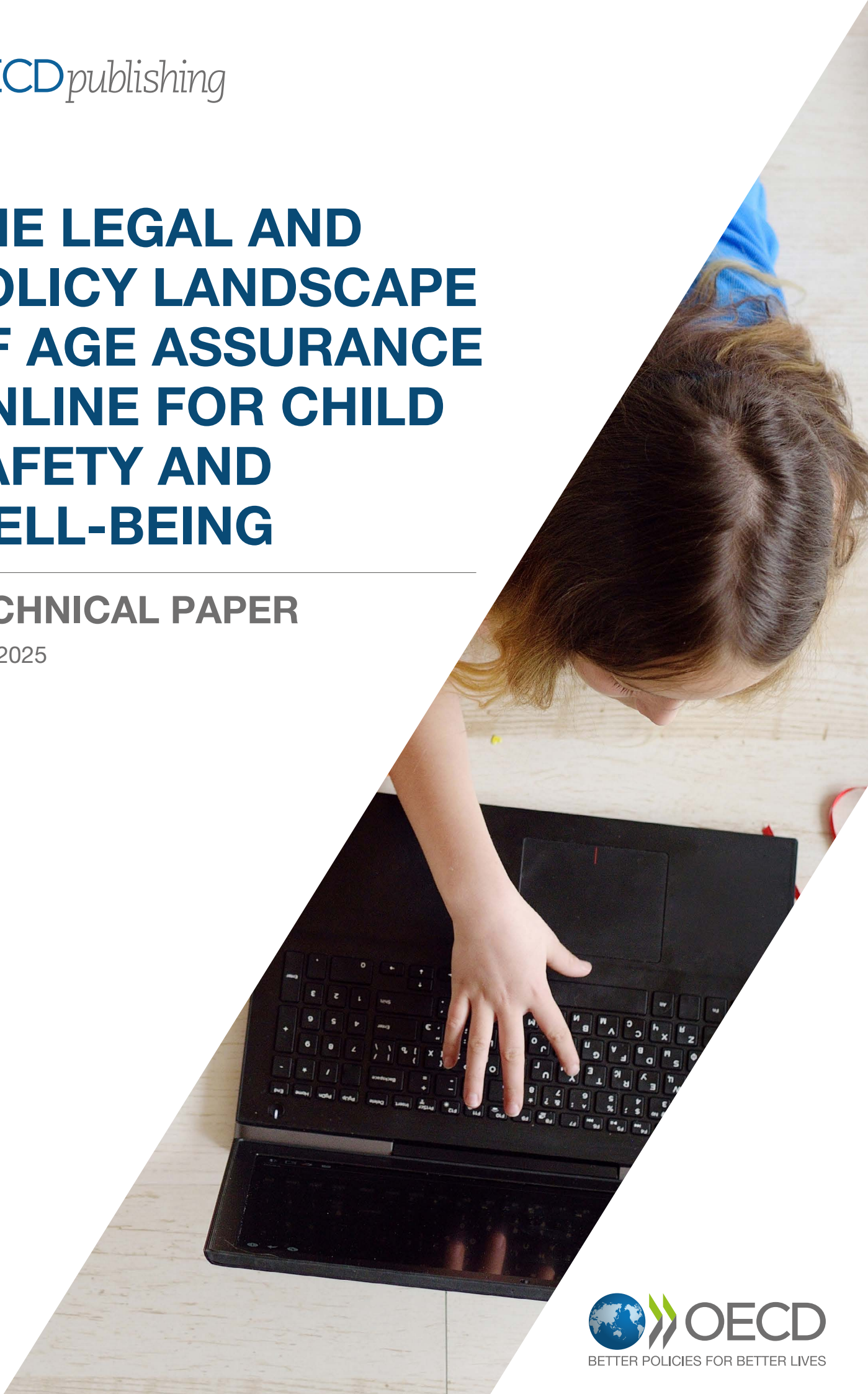
OECD publishing

THE LEGAL AND POLICY LANDSCAPE OF AGE ASSURANCE ONLINE FOR CHILD SAFETY AND WELL-BEING

TECHNICAL PAPER

June 2025



OECD
BETTER POLICIES FOR BETTER LIVES

Foreword

This report maps the current legal and policy landscape for age assurance across OECD Member countries. It analyses laws that establish age-dependent protections or obligations ("age limits") and therefore trigger a need to assure age. It considers laws covering online safety (including on pornography and social media services), privacy and the online sale of age-restricted goods. Together with a companion report benchmarking the age-related policies and practices of 50 online services that children use, this work aims to support government and industry action for promoting the opportunities offered by digital technologies for children while keeping them safe from potential harms and protecting their rights and freedoms.

This report was written by Lisa Robinson, under the supervision of Jeremy West, with support from Nora Beauvais and Aahil Sheikh. Editorial review and assistance for publication were provided by Andreia Furtado. It incorporates feedback from delegates of the OECD Digital Policy Committee (DPC) as well as delegates from its Working Party on Data Governance and Privacy (DGP). This paper was approved and declassified by written procedure by the Digital Policy Committee on 21 May 2025 and prepared for publication by the OECD Secretariat.

Note to Delegations:

This document is also available on O.N.E Members & Partners under the reference code:

DSTI/DPC(2024)25/FINAL

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Cover image: © AnastasiaNi/Shutterstock.com

© OECD 2025

Attribution 4.0 International (CC BY 4.0)

This work is made available under the Creative Commons Attribution 4.0 International licence. By using this work, you accept to be bound by the terms of this licence (https://creativecommons.org/licenses/by/4.0/).

Attribution – you must cite the work.

Translations – you must cite the original work, identify changes to the original and add the following text: In the event of any discrepancy between the original work and the translation, only the text of original work should be considered valid.

Adaptations – you must cite the original work and add the following text: This is an adaptation of an original work by the OECD. The opinions expressed and arguments employed in this adaptation should not be reported as representing the official views of the OECD or of its Member countries.

Third-party material – the licence does not apply to third-party material in the work. If using such material, you are responsible for obtaining permission from the third party and for any claims of infringement.

You must not use the OECD logo, visual identity or cover image without express permission or suggest the OECD endorses your use of the work.

Any dispute arising under this licence shall be settled by arbitration in accordance with the Permanent Court of Arbitration (PCA) Arbitration Rules 2012. The seat of arbitration shall be Paris (France). The number of arbitrators shall be one.

Executive summary

"Age assurance" is an umbrella term describing approaches for determining which online users are children, to ensure they are offered age-appropriate services tailored to their needs and that they are protected from illegal, adult, or otherwise harmful content or services. This paper surveys the legal and policy landscape for age assurance online in OECD Member countries. It considers laws that establish age-dependent protections or obligations ("age limits") and therefore trigger a need to establish age, aiming to provide clarity on those laws and related policies. To do this, it groups age assurance laws and policies into three broad categories:

- **Age-appropriate service delivery.** These concern provisions relevant to online services with a mixed-aged audience and are most often found in online safety laws, but also appear in laws specific to social media. These laws do not seek to prevent a child from accessing a service altogether, but rather require protections for users in certain age cohorts, or in response to certain risks.
- **Hard age limits.** These concern legal frameworks that set an age limit below which access to certain products and services is prohibited. These are: i) laws regulating access to pornography online; ii) age rating frameworks for online content; and iii) laws relevant to the online purchase of age-restricted goods.
- **Privacy and data protection legal frameworks.** These concern age limits relevant to consent for processing personal data, special protections for children's data and protections regarding targeted advertising.

The main findings are:

General observations

- The legal landscape is complicated. It is often unclear when and what age limits apply, under which legal regime (e.g. safety or privacy) an age limit exists, how age limits from different legal regimes interact, or how age limits covering the same legal regime vary across borders. The same service may be subject to several age limits and consequent age assurance requirements that arise under different laws aimed at addressing different risks.
- Age assurance requirements can be ether "express" or "implied". Both have equal force, but express age assurance requirements overtly state that the use of an age assurance mechanism is mandatory. Implied requirements are unstated but can be inferred from a need to determine which users are children in order to respect age limits. Additionally, some laws provide exceptions to age assurance requirements, meaning that services may be able to implement alternate measures to safeguard the interests of children and thereby avoid a need to assure age.

Age assurance for age-appropriate service delivery

- These requirements arise in online safety laws that broadly apply to services with a mixed age user-base and exist in 28 OECD Member countries. Some have express requirements while

© OECD 2025

others contain implied requirements, but they all apply to children broadly (i.e. to all persons under 18). Australia, the European Union and the United Kingdom are developing enforceable implementation guidance that may create express requirements for different age cohorts. These requirements most often apply to "harmful content", although not all countries define that term.

- While concerns about social media can be addressed through broader online safety laws, there is a trend of express age assurance requirements being enacted to specifically regulate children's access to social media. Provisions range from those that prevent children from opening accounts altogether, to prohibiting platforms from serving children algorithmically curated feeds or frequent notifications. Three OECD Member countries are considering legislation that would establish social media specific age limits and one has passed a law, as have several US states[1].

Age assurance to enforce hard age limits

- Children across the OECD have uneven protections regarding access to pornography. While all OECD Member countries have a law to prohibit children's access to pornography generally (i.e. without specifying online or offline), only 23 have a law specifically prohibiting children's access to pornography online. Only five of those laws include a detailed age assurance requirement. Seven of the 23 countries do not mention a need to assure age to comply with their law, and the others describe their age assurance requirement in vague terms.
- There are very few legal protections preventing the purchase of age-restricted goods online. Only a few OECD Member countries have laws that expressly require online age assurance and those that do lack specificity.
- Classification rating schemes play a significant role in setting recommended age ratings, but they are not necessarily supported by research or clinical knowledge on child development and processes for granting ratings lack transparency and accountability.

Age assurance for data protection and privacy

- Age limits are most uniformly expressed in privacy and data protection laws that create similar protections for children across the OECD. Twenty-seven OECD Member countries have legal provisions requiring special protection for children's data. Thirty-three have provisions requiring parental consent to process such data. Age limits differ across the two privacy measures of special protection and parental consent. Special protection applies to users under 18 in 26 OECD Member countries, and to users under 13 in one. Ages for requiring parental consent are highly variable and range between 13 and 18.

Guidance for implementing age assurance requirements

- A lack of specificity on how to comply with age assurance requirements is common across the laws analysed. These requirements are often only implied, described in tech-neutral language, or a non-exhaustive list of potential methods is given. In several OECD Member countries, however, implementation guidance for age assurance is emerging.
- Online safety and privacy regulators are focused on age assurance, setting up working groups, providing targeted advice and in at least one case proposing their own technical solutions.

© OECD 2025

Table of contents

© OECD 2025

Tables

Boxes

© OECD 2025

1 Introduction

Legal age limits have long prohibited children's[2] access to information, goods, services, commercial practices, and spaces that can harm them, or that they do not have the capacity and maturity to experience safely. Children are, for instance, typically barred from casinos. Goods such as alcohol and cigarettes routinely require a date of birth check before they can be purchased, and advertisements for them are often restricted to times and places that suppose an adult audience. Alongside strict age requirements, classification and age rating systems have been providing guidance on whether movie and games are suitable for children since well before games existed online and movies could be purchased, downloaded, or streamed.

Digital technologies have brought easy and expanded contact between individuals and dissemination of content across the globe. They provide for the easy purchase of goods that may have previously been limited by geographical or financial constraints (OECD, 2022[1]). While these facets of digital transformation have brought benefits for children in many ways, they have also exposed them to risk, including by rendering many traditional age-dependent safeguards unenforceable or unworkable. There is, for instance, limited value in restricting pornography to "adults only" when a child can access it instantly online with a simple and unverified answer of "yes" to the question of whether they are over the age of 18.

As well as affecting the efficacy and suitability of traditional age-based safeguards to protect children from certain harms, digital transformation has reshaped the risk landscape for children. Children today live many aspects of their lives online (e.g. leisure, play, education and social connection) and the digital spaces they inhabit present a wide spectrum of risks to which children are more vulnerable than adults. Online, children can be exposed to harmful or illegal content, bullied, harassed, or sexually exploited and abused, among other dangers (OECD, 2021[2]) (OECD, 2023[3]) (OECD, 2024[4]). Increasingly, there are concerns that children may be harmed not just by what they see or who contacts them online, but by the very design or use of certain services. Together with these risks, the pervasive use of data underlying the business models of many digital products and services children use has created new privacy and consumer risks for children (OECD, 2021[2]) (OECD, 2024[5]).

It is in this context that major stakeholders, including policymakers, are paying increased attention to the need for effective age assurance tools and mechanisms to safeguard the rights and interests of children online. Their concern, however, is not only to protect children from harm, but also to underpin the delivery of age-appropriate experiences that support children's development and advance their well-being (OECD, 2023[6]).

Developing and implementing age assurance laws and policies is not a simple task. While many of the methods that have been used to establish a person's age online to date (e.g. self-declaration) are ineffective (Smirnova, Livingstone and Stoilova, 2021[7]), the capacity of more advanced age assurance solutions (such as the use of biometrics or profiling) to be accurate, effective and privacy preserving needs to be demonstrated. For instance, some solutions require significant amounts of data to be collected and/or processed, raising data protection concerns. Other privacy worries, such as surveillance and the loss of freedom to anonymously access websites, can come into play when age assurance is applied to all users of certain websites (e.g. pornography) (Open Rights Group, 2023[8]). Attention must also be given to how best to respect and foster children's developing need for autonomy when considering parental[3] involvement in assuring age, or indeed how best to raise awareness with children and parents of the

© OECD 2025

purpose and utility of age assurance. Research has shown that many parents admit helping their children to circumvent age assurance requirements, often because they simply do not understand its purpose beyond barring children from obviously adult spaces (Revealing Reality, 2022[9]). Additionally, a risk of regulatory fragmentation arises should laws and policies on this issue proliferate and diverge across borders.

This paper is part of a group of research papers the OECD is producing on age assurance. A concurrent report benchmarks industry practices (OECD, 2025[10]). It is intended that these two reports be followed by others analysing: i) technical age assurance solutions; and ii) the age-appropriateness of current age limits and age recommendations for digital services and products commonly used by children. The purpose of this paper is not to provide policy recommendations, but rather to offer an objective snapshot of the current (and often fragmented) legal landscape for age assurance. It serves as a companion to the paper benchmarking industry practices, as well the two envisaged future papers. The findings of which will all need to be considered in light of the applicable laws.

This research is undertaken in the context of the OECD's Recommendation on Children in the Digital Environment (the Recommendation), which provides guidance to governments and other stakeholders for fostering a safe and beneficial digital environment for children. Relevant to age assurance, the Recommendation calls on governments to foster "the research, development, and adoption of privacy protective, interoperable and user-friendly technologies that can restrict contact and access to content that is inappropriate for children, taking into account their age, maturity, and circumstance" (at III.5) (OECD, 2021[11]). Additionally, Guidelines for Digital Service Providers[4] adopted by the OECD Council alongside the Recommendation state that digital service providers should ensure that they respect any requirements in laws and policies to implement age-based restrictions aimed at protecting children, and that the measures they implement should be proportionate to risk and privacy preserving (at 1.d) (OECD, 2021[12]). This research also provides further context to the 2024 report "Towards Digital Safety by Design for Children", which identifies age assurance as a key component in implementing a safety by design approach for children on digital products and services (OECD[5]).

Methodology and scope

This paper maps laws across the OECD that require digital service providers to implement age assurance to provide certain protections to children. This includes laws that i) expressly require age assurance (express requirements), or ii) imply a need for age assurance to be effectively enforced (implied requirements)[5]. The latter means laws mandating safeguarding measures for children that can only be effective if the digital service provider knows which of its users are children.

Legislative action for age assurance is fast moving and concurrent with the development of soft measures such as guidance documents. Therefore, simply considering laws that are already in force does not give a complete picture of the current intensive policy action driving age assurance as a key lever in safeguarding the rights and interests of children online – nor a picture of the age assurance regulation that is likely on the horizon. Accordingly, where appropriate, this paper also considers policy and guidance documents issued by authorities in OECD Member countries that call for age assurance, as well as proposed laws that envisage an age assurance provision.

Desk research helped to identify relevant laws and policy measures in OECD Member countries. A series of tables in Annexes A – E set out the relevant requirements in these laws and policies. The following categories are considered:

- **Age-appropriate service delivery**. This concerns laws which require digital service providers to put in place protections for children on services with a mixed age user base. Such laws don't seek to prevent a child from accessing the service altogether, but rather require that the digital

© OECD 2025

service provider puts in place protections for users from certain age cohorts. These provisions are largely found in online safety laws, however there are a number of emerging frameworks covering social media in particular and so these laws are specifically examined. The relevant tables are:

- Age based protections and age assurance requirements in online safety laws and policies (Table A A.1); and
- Age based protections and age assurance requirements relevant to social media (Table A B.1).

- **Hard age limits**. These are found in legal frameworks relevant to preventing children accessing a service or product via online means in which the law establishes a hard age below which children should not have access. These include: i) laws regulating access to pornography online; ii) age rating frameworks for online content; and iii) laws relevant to the purchase of age-gated goods (i.e. alcohol, cigarettes and knives) via online means. The relevant tables are:
  - Age based protections and age assurance requirements relevant to accessing pornography (Table A C.1); and
  - Age limits and age assurance requirements in laws regulating sale of alcohol (Table A E.1). cigarettes (Table A E.2), and knives (Table A E.3).
- **Privacy and data protection** legal frameworks. These are laws that: i) set an age limit for consent to data processing; ii) establish special protection for children's data; and iii) protect children from targeted or behavioural advertising. The relevant table is:
  - Age based protections and methods for enforcing them in privacy and data protection laws (Table A D.1Table A D.1).

The information compiled in the tables has informed this paper, providing a picture of several important considerations for age assurance, including: when it is expressly called for, and when it is implied; the reasons to assure age (e.g. for privacy or safety); the inclusion of age assurance as a measure for safeguarding children in policy or guidance documents; and emerging legislation that is likely to include an age assurance requirement.

Not every law or policy relevant to safeguarding the needs and interests of children online is included in this report. Likewise, not all child safety-relevant provisions of online safety laws are included. Instead, the paper focuses on provisions that expressly call for age assurance (express requirements) or, without overtly saying so, necessitate investigating whether a user is a child to be appropriately applied and enforced (implied requirements). Provisions that cover issues such as filtering tools[6], complaint mechanisms, content moderation, or parental controls are only addressed if they are drafted in a way that requires a need to determine if a user is a child as a threshold for their application.

A note on sub-national laws

OECD research usually focuses on initiatives at the national level only. However, given a surge of legislative action on age assurance at the state level in the United States, and its consequent relevance to the overarching age assurance landscape state-level laws from the United States are included in this research. These laws are relevant because global companies operating in these sub-national jurisdictions must comply with these requirements, just as they must comply with requirements in the relevant national laws of countries in which they operate. From the companies' point of view, applicable laws all impose responsibilities regardless of whether they are national, sub-national, or supra-national (e.g. EU) laws.

Across the United States in 2023, some 144 bills encompassing age assurance requirements were introduced at state level (Tech Policy Press, 2023[13]). In 2024, a further 57 were introduced (Free Speech Coalition, 2025[14]), and this pattern has continued into 2025 (Lexis Nexis Insights, 2025[15]). This legislative action is focussed on access to social media and pornography. In total, 32 such laws are in force (as of

© OECD 2025

March 2025), all enacted between 2023 and early 2025. To accurately reflect the complex and fast-moving age assurance landscape, of which this legislative action forms a part, these laws are set out in the tables in the annexes and, where appropriate, considered in this report. The trend of sub-national jurisdictions enacting laws mandating age assurance is not observed in other OECD Member countries.

The paper first provides scene setting considerations relevant to understanding age assurance, including key terminology, trends and an overview of the different risks age assurance requirements address. It then maps age limits and age assurance requirements that arise in laws relevant to age-appropriate service delivery, hard age limits, and privacy and data protection. After a brief conclusion, annexes to the report presents details of the relevant laws across the three different categories.

© OECD 2025

2 Scene setting

What is age assurance?

Age assurance refers collectively to approaches used to determine whether an individual is a child (or a child from a certain age cohort) to ensure they are i) offered online services that are age-appropriate and tailored to their needs; and ii) protected from adult, harmful or otherwise inappropriate online content or services. Age assurance approaches take several different forms but can be broadly divided into those technologies or mechanisms that estimate a user's age or age range, and those that verify the user's actual age. Different terms commonly used in relation to age assurance are set out in Box 2.1.

Box 2.1. Age assurance terminology

Age assurance is an umbrella term encompassing the different processes used to verify or estimate the age, or age range, of an individual. Both age estimation and age verification are types of age assurance.

Age estimation refers to processes to establish the likely age of a user, or the likely age range of a user. These processes include automated analysis of behavioural or environmental data, observing how a user interacts with a device or with other users, using metrics derived from motion analysis, testing the user's capacity or knowledge, and biometric classifiers.

Age gating refers to technical measures to restrict or block access for users that do not meet an age requirement.

Age limit refers to the upper bound of the age range to which a legal protection applies.

Age verification occurs when a user's age (and often exact date of birth) is established by verifying their identity against official documents. Age verification relies on hard identifiers (e.g. a government-issued ID document) or verified sources of identification (e.g. a credit card). While such processes can be used to establish a person's full identity (e.g. name, address and date of birth), they may also be used to establish age only.

Self-declaration occurs when a person is granted access to an age-gated website merely by declaring that they meet the age requirement. This is usually done by entering a birthdate or ticking a box.

Verified parental consent occurs when a parent verifies their identity using an official document to provide consent for their child to use a service, or for the processing of their child's data. This is necessary when a child has not yet reached the legal age of capacity to consent to a service's Terms of Service, or to the processing of their data.

Sources: (5Rights Foundation, 2021[16]) (Australian eSafety Commissioner, 2022[17]) (Government of the United Kingdom, 2023[18]) (United States Code of Federal Regulations, 2013[19]).

© OECD 2025

Efficacy of age assurance practices

While age restrictions on accessing certain services and sites are not new, as risks for children associated with digital services have grown, it has become apparent that current age assurance practices are failing to protect children in each of the three categories analysed in this report (as outlined under Methodology and scope).

In 2021 research found that across the European Union age assurance mechanisms are rarely implemented for the sale of age-restricted goods, and barriers to accessing age-restricted content, goods and services are mostly ineffective (Smirnova, Livingstone and Stoilova[7]). Privacy age limits have likewise often proven to be ineffectively applied, and many examples exist of privacy enforcement authorities sanctioning digital service providers for failing to respect these limits. This includes examples of both failing to obtain relevant consent to process children's data (United States Federal Trade Commission, 2022[20]), and failing to put in place special protections for children's data (United Kingdom Information Commissioner's Office, 2024[21]). Delivering an age-appropriate experience requires knowing an account holder's correct age and, sometimes, when that account holder is a child, preventing their access. Here, too, age assurance practices have often failed. For instance, despite many social media services prescribing an age of 13 or above, research shows that children below this age regularly hold accounts (United States Public Health Service, 2023[22]) (Rideout et al., 2022[23]) and commonly their user age does not match their real age, leaving them without the age-based protections that services sometimes tie to a user's account age (Ofcom, 2022[24]).

Calls for more effective age assurance and related activity have intensified in recent years. In addition to the OECD's Recommendation on Children in the Digital Environment (OECD, 2021[11]), the Committee on the Rights of the Child, for instance, specified that "robust age verification systems should be used to prevent children from acquiring access to products and services that are illegal for them to own or use" (2021[25]). In addition, guidelines from the Council of Europe specify that "States should require the use of effective systems of age-verification to ensure children are protected from products, services and content in the digital environment which are legally restricted" (2018[26]).

Civil society, industry and international networks of regulatory bodies have taken action, as well. For instance, the WeProtect Global Alliance[7] in conjunction with the Centre for Information Policy Leadership[8] have been leading a series of multistakeholder conversations aimed at bringing the privacy and safety communities together to discuss challenges related to age assurance (2024[27]). On the industry side, in late 2023, the Digital Trust and Safety Partnership (an industry consortium) developed guidance on best practice and principles for age assurance (2023[28]). Privacy enforcement authorities have formed an International Age Assurance Working Group, which invites collaboration with online safety regulators and which in 2024 published a joint statement on a common international approach to age assurance (International Age Assurance Working Group[29]). Online safety regulators have likewise come together to establish an age assurance working group (Global Online Safety Regulators Network, 2024[30]) and a group of European-based online safety and media regulators formed a working group on the topic in 2023 (Ofcom[31]).

Alongside these developments, several independent providers have been developing technical age assurance methods. The Age Verification Providers Association lists (as of March 2025) 29 age assurance providers that offer 13 types of products across ten sectors (Age Verification Providers Association, 2025[32]), the IEEE has developed a standard and the ISO is in the process of doing so (Age Verification Providers Association, 2025[33]).

© OECD 2025

What risks do age assurance mechanisms address?

A significant complication in implementing age assurance requirements is the overlapping nature of risks to children from digital products and services, and consequently the overlapping nature of legal protections aimed at addressing the risks. Different laws address different concerns that can all be present on one product or service. For instance, a social media service may need to comply with age limits and age assurance requirements relevant to protecting children's privacy, keeping them safe and ensuring that they are not the subject of targeted advertising.

To demonstrate this complexity, take for instance an online game that:

- collects data;
- serves advertisements;
- operates an interactive chat feature, where users have been known to share information about eating disorders and engage in bullying – but operates default settings to prevent certain age cohorts from having access to this feature;
- has a mild level of violence in the game itself; and
- can offer in-game purchases – but also offers the ability to turn off this feature.

Imagine that such a service operates in a jurisdiction that:

- rates the main content of the game as suitable for children 13 or older, as part of a classification scheme;
- requires parental consent to process the data of persons under 15, under a privacy law;
- requires special protection for children's data, being all persons under 18, under a privacy law;
- prohibits the profiling of persons under 18 for the purpose of serving them targeted advertising, as a result of provisions in both privacy and online safety laws;
- prohibits children from participating in a game with in-game purchase capacity, due to a provision in an online safety law;
- prescribes an enforceable age assurance requirement to ensure that persons under 18 cannot encounter information promoting an eating disorder, due to a provision in an online safety law; and
- establishes age assurance as one possible mitigation measure for preventing children from encountering bullying content, due to a provision in an online safety law.

Therefore, the provider of this game that is ostensibly rated as suitable for a 13-year-old child, would still need to determine if each user is:

- younger than 15 for the purpose of knowing if parental consent is needed to process data;
- younger than 18 to establish protections on their personal data and to prevent profiling for the purpose of targeted advertising;
- younger than 18 for the purpose of ensuring that the proper defaults are engaged relevant to the chat feature and in game purchases;

And, then determine whether age assurance is an appropriate method for mitigating the risk of a child being bullied. Simply determining if a user is over 13 would be insufficient. A 17-year-old user for example, may not need any protections relevant to the game's content or consent to data processing, but all the latter examples would apply.

© OECD 2025

3 Age-appropriate service delivery

This section considers laws that aim to ensure age-appropriate experiences for children on services that have a mixed user-base[9] (i.e. both children and adults). It examines i) the scope and parameters of provisions in online safety laws) and ii) the particular case of social media, which has been the subject of much attention from policymakers.

Online safety requirements

What are the relevant laws and age limits?

Age limits and express age assurance requirements are found in a number of specific online safety laws, with many arising from the implementation of the European Union's Audiovisual Media Services Directive (AVMSD) (2018[34]) (see further explanation of the AVMSD in section 4). Jurisdictions with such laws, the types of services to which they apply, the type of content they seek to regulate and their reasons for doing so are set out in Table 3.1.

Table 3.1. Express age assurance requirements in online safety laws

Jurisdiction	Type of service	Type of online content	Purpose of AA requirement
Austria*	Video sharing platforms	Material that may impair the physical, mental or moral development of minors, explicitly including gratuitous violence.	Prevent access to under 18s
Belgium*	Video sharing platforms	Material that may impair the physical, mental or moral development of minors, explicitly including gratuitous violence.	Prevent access to under 18s
Czech Republic*	Video sharing platforms	The most objectionable content that may impair the physical, mental or moral development of minors, explicitly including gross self-inflicted violence.	Prevent access to under 18s
Denmark*	Video sharing platforms	Material that may impair the physical, mental or moral development of minors.	Prevent access to under 18s
EU (AVMSD)	Video sharing platforms	Material that may impair the physical, mental or moral development of minors. The most harmful content (i.e.) gratuitous violence is to be subject to the strictest measures.	Prevent access to under 18s
EU (DSA)	VLOPs / VLOSEs	Material identified pursuant to a s34 risk assessment, as presenting a risk.	As part of appropriate measures to prevent risks to under 18s
France* (Leotard Law)	Video sharing platforms	Material that may harm the physical, mental or moral development of minors.	Prevent access to under 18s
France* (SREN Law)	Online games	Monetiseable digital objects on online games.	Prevent under 18s participating in such online games
France* (Penal Code)	Online platforms generally	Material that is: - violent - incites terrorism - pornographic images involving animals - likely to undermine human dignity; or	Prevent access to under 18s

© OECD 2025

Jurisdiction	Type of service	Type of online content	Purpose of AA requirement
		- like to incite children to engage in physically dangerous games.	
Germany*	Video sharing platforms (which are not subject to the DSA)	Content detrimental to children's development, which includes gratuitous violence, and content that is excessively frightening, advocates violence or may impair socio-ethical values.	Prevent access to under 18s
Greece*	Video sharing platforms	Material that may have a negative effect on the physical, mental or moral development of minors. The most harmful content includes gratuitous violence.	Prevent access to under 18s
Hungary*	Video sharing platforms	Content capable of harming the physical, intellectual, spiritual or moral development of minors.	Prevent access to under 18s
Iceland*	Video sharing platform	Material that may harm the physical, mental or moral development of minors, in particular gratuitous violence	Prevent access to under 18s
Ireland*	Online platforms / Video sharing platforms	"Age-inappropriate content", meaning: • content that is likely to be unsuitable for children (either generally or below a particular age); and • including, in particular, content consisting of realistic representations of, or of the effects of, gross or gratuitous violence or acts of cruelty.	Prevent access to children having regard to their capabilities, their development, and their rights and interests.
Italy*	Video sharing platforms	Material that may harm the physical, mental or moral development of minors, including gratuitous, or persistence or brutal violence.	Prevent access to under 18s
Korea (Youth Protection Act)	Any person providing material harmful to youth	Material harmful to youth as defined by a separate decree.	Prevent access to under 19s
Korea (Youth Protection Act)	Online games	An online game account.	To seek parental consent for under 16s to open account
Lithuania*	Video sharing platforms	Material that has a negative impact on minors physical, mental or moral development, especially gratuitous violence.	Prevent access to under 18s
Luxembourg*	Video sharing platforms	Material that may harm minor's physical, mental or moral development.	Prevent access to under 18s
Slovak Republic*	Video sharing platforms	Content that may disturb the physical, psychological or moral development of minor's, including gross unjustified violence.	Prevent access to under 18s
Slovenia*	Video sharing platforms	Content that may harm a child's physical mental or moral development, including gratuitous violence	Prevent access to under 18s
Spain*	Video sharing platforms	Material that may harm minor's physical, mental or moral development, particularly the most harmful content which includes gratuitous violence	Prevent access to under 18s
Switzerland	Platform services (in the areas of film and video games)	Material that may impair the physical, mental, psychological, moral or social development of minors	Prevent access to under 18s
United Kingdom	Regulated user-to-user services hosting primary priority content	Prevent children's access to content that encourages or promotes or provides instructions for: suicide; deliberate self-injury; and eating disorders.	Prevent access to under 18s

Note: EU and EEA Member States that are subject to the provisions of the AVMSD are denoted with "*". EU/EEA laws also routinely explicitly reference pornography as "most harmful content", as is addressed in section 4. The relevant provisions in United Kingdom law regarding pornography are likewise addressed in that section.
Source: Table A A.1. Age-based protections and age assurance requirements in online safety laws and policies

Outside of Korea, the United Kingdom and the requirement in the DSA, the above age assurance requirements all arise from the AVMSD[10]. The DSA establishes a regulatory framework for online safety in the EU/EEA, and the requirement mentioned in Table 3.1 obliges very large online platforms (VLOPs) and very large online search engines (VLOSEs) to assure age when a risk to children has been identified on their platform pursuant to a statutory risk assessment (European Commission, 2022[35]).

The laws stemming from the AVMSD, while mostly uniform, have slight differences in how they describe content that is harmful to minors, and not all specify that gratuitous violence is included – despite it being

© OECD 2025

mentioned in the AVMSD. For the most part, these laws reference age assurance as one possible appropriate measure for preventing children's access to harmful content. In addition, under the AVMSD, video sharing platforms (VSPs) fall under the jurisdiction of a country's regulator when that VSP is established in their jurisdiction. This means that while some of the countries mentioned above may have an age assurance requirement in their law, there may be no VSPs in their jurisdiction that are bound by it (European Commission, 2018[34]) (European Audiovisual Observatory, 2023[36])[11].

Within the OECD, Korea's law presents the most clearly stated age assurance requirement and establishes an unequivocal obligation to assure age to prevent children accessing harmful material. The United Kingdom's law is the most specific in the sense that it states exactly what amounts to harmful content from which children should be protected. This law, however, does provide for other mitigating measures that would nullify the need to assure age, including the digital service provider prohibiting the content.

In some legal frameworks, protections for children do not expressly require age assurance but do imply a need to know if a user is a child for the purpose of implementing safeguards. These are set out in Table 3.2.

Table 3.2. Implied age assurance requirements in online safety laws

Jurisdiction	Type of service	Type of online content	Purpose of AA requirement
Australia	Services that: • Enable end-users to search for or communicate with other end-users; • Interactive gaming services; • Designated high risk internet services.	• Illegal content; • Crime, violence or drug related material; • Online pornography depicting specific fetishes or fantasies.	For all such services: • Set the account of a young Australian child (**<16**) at private by default. • Not allow an end-user to know the location of a young Australian child end-user (**<16**) without their parent's consent. For designated high-risk services: • Ensure that an Australian child (**<18**) known by the service to be a child does not become an end-user • Prevent an Australian Child (**<18**) accessing the service.
EU (DSA)	Online platforms accessible to minors	Requirement to put in place a high level of privacy, safety and security for minors.	Protection of minors
Finland*	Video sharing platforms	Programs harmful to a child's development due to violent content, or which cause anxiety	Prevent access to under 18s
Korea (Network Act)	Information communication service providers	Inappropriate content in text or voice chat services available to children under 14.	Prevent access to persons under 14
Norway*	Video sharing platforms	Seriously harmful content	Prevent access to under 18s
Poland*	Video sharing platforms	Material that may threaten a child's physical, mental or moral development.	Prevent access to under 18s
Portugal*	Video sharing platforms	Material that may impair a child's physical, mental or moral development.	Prevent access to under 18s
Sweden	Video sharing platforms	Material that contains realistic violence.	Prevent access to under 18s, unless access is justified for a special reason
United Kingdom	Regulated user-to-user services hosting priority content	Priority content, being: • abusive content targeting protected characteristics • content inciting hatred • content encouraging, promoting or providing instructions for an act of serious violence against a	Protect children (<18)

© OECD 2025

Jurisdiction	Type of service	Type of online content	Purpose of AA requirement
		person, or for a challenge or stunt highly likely to result in serious injury • bullying content • content which depicts real or realistic: serious violence or injury against a person, animal or fictitious creature. • content that encourages the consumption of a physically harmful substance.	

Note: EU and EEA Member States that are subject to the provisions of the AVMSD are denoted with "*". EU/EEA laws also routinely explicitly reference pornography as "most harmful content" however this is addressed in section 4.
Source: Table A A.1. Age-based protections and age assurance requirements in online safety laws and policies

Laws vary significantly across the OECD, with the requirements in the United Kingdom and Australia providing the most context regarding who the laws apply to, why and for what content. A number of the requirements in Table 3.2 arise from the AVMSD, but in these, age assurance is not specified as an appropriate measure for preventing children's access to harmful material. The implementation of the DSA may indeed prove to include more specific age assurance requirements and guidance for implementing the relevant protections for children is under development (European Commission, 2024[37]). Likewise, in Australia, codes for managing certain content are developing alongside an age assurance trial (Australia's eSafety Commissioner, 2024[38]), so the eventual requirements may also come with strong age assurance elements that are not currently in the law. The draft versions of these codes (as of March 2025) envisage age assurance requirements for dating and gaming services, and to prevent access to self-harm material (and pornography). The drafts refer to age assurance measures needing to be "technically feasible and reasonably practicable" (Online Safety Australia, 2025[39]).

There are also proposals in two OECD Member countries (the United States and Spain) for online safety laws that would encompass or more strictly enforce age assurance requirements.

What are the age assurance requirements?

The age assurance measures specified in the above laws are set out in Table 3.3.

Table 3.3. Age assurance methods mentioned in online safety laws

Jurisdiction	Government ID	Verifiable e-signature	Personal ID no.	Established Accounts	Detailed Principles	Awaiting Guidance	Does not specify
Austria							•
Belgium							•
Czechia							•
Denmark							•
EU						•	
France						•	
Germany					•		
Greece							•
Hungary			•	•	•		

© OECD 2025

Jurisdiction	Government ID	Verifiable e-signature	Personal ID no.	Established Accounts	Detailed Principles	Awaiting Guidance	Does not specify
Iceland							•
Ireland					•		
Italy						•	
Korea	•	•	•	•			
Lithuania							•
Luxembourg							•
Slovak Republic							•
Slovenia							•
Spain						•	
Switzerland							•
United Kingdom					•		

Notes: "Established accounts" refers to mechanisms that rely on evidence of an existing account in the person's name (e.g. banking, phone, credit card).
Source: Table A A.1. Age-based protections and age assurance requirements in online safety laws and policies.

Within the OECD no law specifies one particular age assurance method that must be used. Korea offers the most restrictive age assurance provision in that: i) it is mandatory and cannot be nullified using another mitigating measure; and ii) it sets a limited number of specific options for assuring age that must be used, rather than suggesting a range of non-mandatory options. Other laws tend to be limited to principles and some give examples of methods that could be used.

When particular methods are not specified, the above laws nonetheless usually require that the solution be "feasible" and/or "proportionate". For example, Denmark's law specifies that this means considering the size and nature of the service, and Hungary's explains that to be effective the solution must actually prevent children from seeing the content. The laws in six OECD Member countries (Czechia, Denmark, Finland, Slovak Republic, Slovenia and Spain) prohibit age assurance solutions from pre-checking of content, filtering, or preliminary control measures. Both Ireland and the United Kingdom require more than self-declaration for age assurance requirements to be met.

Thirteen laws include a provision prohibiting any personal data collected for the purpose of assuring age being used for commercial purposes. Eleven OECD Member countries (Belgium, Czechia, Denmark, France, Greece, Hungary, Ireland, Iceland, Luxembourg, Slovak Republic and Spain) limit this protection to children's personal data (and the protection is drafted in this manner in the AVMSD), and two (Slovenia and Sweden) apply this protection generally to any personal data collected for the purpose of assuring age.

Online safety regulators are elaborating distinct guidance for age assurance, including those in France (ARCOM, 2023[40]), Germany (Kommission für Jugendmedienschutz, 2024[41]), and Italy (European Audiovisual Observatory, 2024[42]). Ireland (Coimisiún na Meán, 2024[43]) and the United Kingdom's (Ofcom, 2024[44]) guidance is provided in codes that support the implementation of their laws. The European Commission established a task force on age assurance in early 2024 (European Commission, 2024[45]); guidance is still forthcoming.

© OECD 2025

Specific social media requirements

What are the relevant laws and age limits?

While certain protections in online safety laws (considered in the subsection directly above) extend across a number of services that encompass social media services, there has been separate legislative action targeted directly at social media. This subsection considers those social media-specific laws, which for the most part emerge at the US state level and are independent of other online safety legal regimes.

Australia, however, is an exception. In late 2024, Australia passed a law requiring social media platforms operating in Australia to take reasonable steps to prevent account creation for Australian children under the age of 16. Australia already had an existing statutory instrument concerning social media services, developed in the context of Australia's Online Safety Act. The new law is due to come into effect in December 2025 and guidance (including the interplay with the existing code) is under development (Australia's eSafety Commissioner, 2025[46]).

Colombia, Spain and the United States are considering targeted social media laws that would set age limits and one of which (the United States) would provide for enforceable age assurance.

Table 3.4 sets out the parameters of social-media-specific laws already in force across the OECD.

Table 3.4. Age assurance requirements relevant to social media services

Jurisdiction	Express / implied requirement	Nature / purpose of requirement
Australia (Social Media Law)	Awaiting Guidance	• Requires an "age-restricted social media platform" to take "reasonable steps" to prevent age-restricted users (**<16)** from having an account. • "Reasonable steps" are yet to be defined
Australia (Industry Code)	Implied	• Prevent an Australian child opening / holding an account if below the **service's minimum age** • For certain services (Tier 1), establish default settings and apply safety tools / functionalities for children (**<16**)
California	Express	• To prevent a child being offered an addictive service (**<18**) • To prevent a child being sent notifications during restricted hours *Age assurance not necessary if service has obtained parental consent or does not have actual knowledge the user is a child.*
Colorado	Express	• To send notifications to child users (**<18**) on cumulative use and about use during restricted hours • To provide child users with health information about social media
Florida	Implied	• Prevent children (**<14**) opening / holding an account • Ensure children (**14,15**) have parental consent to open an account
Georgia	Express	• Prevent children (**<16**) from opening / holding an account • Apply special protections to children *Parental consent is required in addition to age assurance*
Louisiana	Express	• Prevent children (**<16**) from holding an account without parental consent *Age assurance requirement nullified if there is parental consent*
New York	Express	• To prevent a child being offered an addictive service (**<18**) • To send notifications about use during restricted hours *Age assurance not necessary if service has obtained parental consent or does not have actual knowledge the user is a child.*
Tennessee	Express	• Prevent children (**<18**) from opening / holding an account • Provide parent with means to supervise account *Parental consent is required in addition to age assurance*
Texas	Express	• Prevent children (**<18**) opening an account • Prevent "known minors" changing account age • Apply special protections to child accounts
Utah	Implied	• Limit children's (**<18**) use of algorithmically curated social media services • Establish time limits for children

© OECD 2025

Jurisdiction	Express / implied requirement	Nature / purpose of requirement
		• Disable engagement driven design elements for children

Source: Table A B.1. Age-based protections and age assurance requirements relevant to social media.

US state laws in California, Colorado, New York and Utah aim to ensure children are not subjected to "addictive" or algorithmically curated feeds and on limiting notifications to children, especially overnight. Each of these jurisdictions set an age limit of 18, but two (California and New York) allow parents to consent to the child receiving an addictive feed, nullifying a need for age assurance. In these two jurisdictions, a lack of actual knowledge that a user is a child also nullifies a need to put in place the relevant protections against "addictive feeds" and notifications. In Utah, this requirement does not come with an express age assurance requirement, but a separate law from that state dealing explicitly with age assurance is currently under court injunction. California's law additionally has a transparency reporting aspect, requiring services to report annually on the number of child users of an "addictive service", and the number of children for whom time limited controls are not engaged.

Australia's requirements under the statutory code aim to ensure that services do not allow an Australian child to hold an account contrary to the age limit set by the service itself, and the relevant services are required to take reasonable steps to ensure that. They also require certain protective default settings to be put in place for users under 16. The Code does not expressly require age assurance but does imply a need to know the user's age and in calling for reasonable steps be taken to comply with these requirements, the Code specifies that age assurance is an acceptable "reasonable step".

Australia's Social Medial Law from December 2024 provides for a stronger enforcement regime than the Code. It requires social media services to take "reasonable steps" to prevent Australian children under 16 opening an account. As of March 2025, those "reasonable steps" are not explicitly defined to include age assurance, and the law provides that the eSafety Commissioner must formulate guidance on "reasonable steps". Public information from the eSafety Commissioner notes that this guidance is being developed in light of the Commissioner's previous research on age assurance and will also take into account the findings of the age assurance technology trial currently underway (Australia's eSafety Commissioner, 2025[46]) (Age Assurance Technology Trial, 2025[47]). It is also noted, that as well as defining what kind of services are captured by this law (see details in Table A A.1), the law empowers the relevant Minister (in consultation with the Commissioner) to designate or exclude particular services.

The rest of the laws establish an age limit for opening a social media account, and/or set requirements for parental consent to opening accounts. The US state of Florida prevents users under 14 from opening an account and requires parental consent for users aged 14 and 15. This law does not expressly require age assurance.

US states Georgia and Louisiana set the minimum age for opening an account at 16 and expressly require age assurance for this purpose. Georgia's law requires both age assurance and parental consent. It also establishes special protections for children's accounts (concerning targeted advertisements and data minimisation) and requires these protections to apply to all users if the company fails to assure age. The main focus of Louisiana's law is ensuring that users under 16 have parental consent, and if parental consent is obtained it nullifies the need to assure age.

Two US states (Tennessee and Texas) require social media users to be at least 18. In Tennessee, social media companies must both assure age and obtain parental consent. Their law also sets out conditions relevant to confirming the age of existing users and requires that parents be equipped with means to supervise their child's account (i.e. viewing privacy settings and establishing time restrictions). Texas's law aims not just to prevent children from opening accounts, but also to prevent "known minors" from amending their age. It also requires special protections for child accounts.

© OECD 2025

As with the US-state-level laws addressing children's access to pornography (see section 4), laws addressing social media have diverse enforcement mechanisms. As compared with the pornography laws, the social media laws are more likely to be overseen by an administrative body, but in two cases (Texas and Utah) the law gives rise only to a private right of action, and in one case (Florida) both private and administrative redress are available. Texas grants standing to bring a lawsuit exclusively to parents or guardians.

Two other OECD Member countries have relevant frameworks. Denmark's Media Council has published guidance aimed primarily at social media services. While unenforceable, this guidance recommends protections for children on social media relevant to harmful and illegal content, behavioural design features, and time limits for use, and recommends that social media services employ age assurance mechanisms. In 2023, France passed a law setting 15 as the minimum age for holding a social media account and setting requirements for age assurance and parental consent. This law is awaiting EU-level approval, so is not presently in force.

What are the age assurance requirements?

The age assurance measures in the above laws are set out in Table 3.5.

Table 3.5. Legal age assurance methods for social media services

Jurisdiction	Self-declaration	Government ID	Age estimation technology	AI tools	Commercially reasonable efforts	Technically feasible efforts	Awaiting guidance	Does not specify
Australia	•		•	•			•	
California							•	
Colorado	•							
Florida								•
Georgia					•			
Louisiana		•			•		•	
New York					•	•	•	
Tennessee								•
Texas	•							
Utah								•

Source: Table A B.1. Age-based protections and age assurance requirements relevant to social media.

None of the laws specify that a particular age assurance method must be used. Instead, they frequently rely on language such as a method being "commercially reasonable" or "technically feasible" without elaborating on what would qualify. In some cases, no method at all is specified or the relevant administrative body is tasked with developing guidance. Unlike with age assurance methods associated with regulating access to pornography (see Table 4.2), self-declaration is noted as a possible method in a few cases. One of these cases, however, is Australia and that country is in the midst of investigating suitable age assurance methods via a trial (Australia's eSafety Commissioner, 2024[48]). A final report on the outcomes of the trial is anticipated in mid-2025 (Age Assurance Technology Trial, 2025[47]).

© OECD 2025

Three jurisdictions (California, New York and Tennessee) include privacy protections in their law. California and New York specify that any data collected for the purpose of assuring age cannot be retained or processed for a commercial purpose. Tennessee's protection is limited to data retention.

Brief conclusions

Laws containing age limits and age assurance requirements for the purpose of providing an age-appropriate experience can be opaque. Many of them arise from the AVMSD and it is not always clear what counts as material harmful to minors. To date, practices to implement these laws have not proved effective (Smirnova, Livingstone and Stoilova, 2021[7]).

Nonetheless, recent legislative action – such as in Australia, Ireland, the European Union, and the United Kingdom – has sought to regulate more strictly how children are protected on platforms where they are likely to encounter harm. In these cases, however, further clarity will likely come from the final elaboration of codes and guidance on how age assurance should be applied, including the results of the trial being run in Australia. Implementation guidance for the DSA may also serve to provide greater clarity on what is considered harmful material for children in the EU, as compared with the current, somewhat disparate laws that implement the AVMSD.

Social media provides a specific case study. While it is the focus of many US state-based laws, social media should not be considered exempt from applicable protections in wider online safety laws. In any event, the effectiveness and enforceability of laws requiring age assurance on social media will need to be examined over time.

© OECD 2025

4 Hard age limits

This section considers laws that set a hard limit below which a child is prohibited from accessing a product or service. It examines the following three cases: i) children's access to pornography; ii) ratings classification schemes; and iii) e-commerce protections. It does not consider age limits or age assurance requirements on products and services that are intended to have a mixed user base, as those laws are discussed in section 3.

Laws regulating access to pornography

What are the relevant laws and age limits?

All OECD Member countries prohibit children from having access to pornography and can be grouped as follows:

- Prohibits child access to pornography online, requires age assurance for that purpose, and has detailed implementation guidance;
- Prohibits child access to pornography online, requires age assurance for that purpose, but without detailed implementation guidance;
- Prohibits child access to pornography online but without an age assurance requirement; and
- General prohibition of a child being given access to pornography without specificity to the online environment

Table 4.1 shows where each jurisdiction falls within those categories. As can be seen, this is a policy area in which there has been substantial legislative action at the state level in the United States.

© OECD 2025

Table 4.1. Legal provisions prohibiting children's access to pornography

Prohibits online access to pornography, with detailed AA requirement	Prohibits online access to pornography, with AA requirement not detailed	Prohibits online access to pornography with no AA requirement	Prohibits access to pornography, with no online aspect
France	Australia (guidance under development)	Costa Rica	Canada
Germany*	Austria*	Finland*	Chile
Ireland*	Belgium*	Norway*	Colombia
Korea	Czechia*	Poland*	Denmark*
United Kingdom	Greece*	Portugal*	Estonia*
Alabama	Iceland*	Sweden*	Hungary*
Arkansas	Italy* (guidance under development)	Republic of Türkiye	Israel
Florida	Lithuania*		Japan
Georgia	Slovak Republic*		Latvia*
Idaho	Slovenia*		Luxembourg*
Indiana	Spain*		Mexico
Kansas	Texas[12]		Netherlands*
Kentucky	Virginia		New Zealand
Louisiana (*2)			Switzerland
Mississippi			United States (Federal)
Montana			
Nebraska			
North Carolina			
Oklahoma			
South Carolina			
South Dakota			
Tennessee			
Utah			
Wyoming			

*: Denotes EU and EEA Member States that are subject to the provisions of the Audiovisual Media Services Directive (AVMSD).
Source: Table A C.1. Age-based protections and age assurance requirements relevant to accessing pornography.

For the most part, OECD Member countries prohibit persons under 18 accessing pornography. In two cases, pornography is prohibited for the whole population (Japan and Korea). In Korea however, despite pornography being entirely prohibited for everyone, there is additionally a law that prescribes an age assurance requirement specifically to prevent child access to pornography. Five countries, as part of their criminal law, prohibit selling, distributing or making pornography available to persons under 16 (Denmark, Estonia, Luxembourg, Switzerland and the United States). Two of these five countries, however, have laws addressing online access to pornography by children above the age of 16 and below 18). Estonia's media regulation law prohibits online access to pornography for persons under 18, and US federal law works alongside the 20 state-level laws regulating online access to pornography, all of which set an age limit of 18.

EU/EEA countries present a somewhat complex picture because they are required to transpose the AVMSD (European Commission, 2018[34]) into their national legal frameworks. The AVMSD provides that Member States ensure that VSP providers take appropriate measures to protect children from harmful content. The most harmful content, which includes pornography, is to be subject to the strictest access controls measures and the AVMSD expressly provides that that includes, as appropriate, establishing and

© OECD 2025

operating age verification systems. The phrasing of the AVMSD, while clearly stating that age verification would be an acceptable measure for meeting its requirements, does not go so far as to demand age verification processes. EU/EEA countries have some flexibility in how they transpose EU Directives but must incorporate the Directive's provisions in their national law in a manner which meets the Directive's aim (European Union, 2025[49]). Countries have implemented the AVMSD in varied ways:

- Two countries expressly regulate VSP activity regarding pornography, require age assurance and elaborate detailed guidance on meeting this requirement.
- Eleven countries have laws that both regulate the activities of VSPs regarding pornography and specify age verification as an "appropriate measure" without elaborating on how the age verification requirement might be met in practice. One of those countries (France) published detailed guidance on age assurance in late 2024 and has a separate law covering pornography online (the SREN law), and another (Italy) is in the process of developing such guidance.
- Five countries specify pornography as the "most harmful content" for children in their law implementing the AVMSD but do not specify age verification as an appropriate measure for protecting children.
- Six countries, while specifying that VSPs must take appropriate measures to protect children from harmful content, do not specify that this relates to pornography or that age verification may be considered an appropriate measure.

The US state laws mostly include detail on how age assurance requirements can be met on the face of the laws. France, Germany, Ireland, Korea and the United Kingdom also set out detailed requirements, albeit in separate guidance documents (Korea's guidance is in a specific Decree). Among the jurisdictions that fall into the second category in Table 4.1, Australia and Italy are in the process of developing guidance. Australia is drafting industry codes, which (as of March 2025) envisage age assurance requirements to prevent children's access to pornography, and which refer to age assurance measures needing to be "technically feasible and reasonably practicable" (Online Safety Australia, 2025[39]). Additionally, as of March 2025, Australia's eSafety Commissioner is running an age assurance trial (Age Assurance Technology Trial, 2025[47]). Since the end of 2024, age assurance is now mandatory on pornographic sites in France, provided they fall under the jurisdiction of the regulator[13] and sites that fail to assure age can be subject to financial sanctions, blocking and de-listing (Arcom, 2025[50]).

While most of the laws listed above are under the administrative responsibility of a government authority (i.e. media regulator, online safety regulator, or justice department), the US state-based laws vary in terms of their enforcement mechanisms and often give rise only to a private cause of action (i.e. the laws entitle a private person, as opposed to the state, to enforce rights under a statute). Some of these laws are enforceable through both civil penalties and private actions for monetary damages. One jurisdiction (Louisiana) has two laws with like provisions, but one creates the possibility of a civil penalty and the other enables private claims.

It is noted that the laws mentioned above are primarily directed at online services whose primary business is the offer of pornographic content. Services on which pornography is accessible but for whom it is not their primary business activity are not captured by these laws and are more likely to fall under the scope of those laws set out in section 3. While children do of course find pornography on websites whose primary business is the offer of pornography, children also frequently find it on other platforms. For instance, one study found that Twitter (now X) was a more common source of pornography for children than dedicated adult websites and another ranked social media as the second most popular source for pornography (behind dedicated websites). Other sources include video streaming platforms, subscription sites, and livestreaming sites (British Board of Film Classification, 2020[51])

© OECD 2025

What are the age assurance requirements?

A range of suggested mechanisms or approaches exist in jurisdictions that specify an age assurance requirement (see the first two columns in Table 4.1). These are set out in Table 4.2.

Table 4.2. Age assurance methods for preventing access to pornography mentioned in laws

Jurisdiction	Government ID	Verifiable e-signature	Established account	Digitised ID	Commercially reasonable methods	Commercially available database	3rd party provider	Detailed principles	Awaiting guidance	Not specified
Alabama					•					
Arkansas	•			•	•					
Australia									•	
Czechia										•
EU										•
Finland										•
Florida					•					
France								•		
Georgia	•			•	•					
Germany								•		
Greece										•
Iceland										•
Idaho	•			•	•					
Indiana				•	•		•			
Ireland								•		
Italy									•	
Kansas					•	•				
Kentucky	•				•					
Korea	•	•	•							
Lithuania										•
Louisiana	•			•	•					
Mississippi	•			•	•					
Montana	•			•	•					
Nebraska	•		•	•	•					
North Carolina					•	•	•			
Oklahoma				•	•	•				
Slovak Republic										•
Slovenia										•
South Carolina				•	•	•	•			

© OECD 2025

Jurisdiction	Government ID	Verifiable e-signature	Established account	Digitised ID	Commercially reasonable methods	Commercially available database	3rd party provider	Detailed principles	Awaiting guidance	Not specified
South Dakota	•		•							
Spain										•
Sweden										•
Tennessee	•				•					
Texas					•					
United Kingdom			•	•				•		
Utah				•	•	•	•			
Virginia					•	•				
Wyoming	•		•							

Notes: "Established accounts" refers to mechanisms that rely on evidence of an existing account in the person's name (e.g. banking, phone, credit card).
Source: Table A C.1. Age-based protections and age assurance requirements relevant to accessing pornography.

None of the above laws specify a particular age assurance method that must be used. Rather, they tend to provide a non-exhaustive list of methods that would be acceptable. The US state-level laws generally call for digitised ID, government ID or a commercially reasonable method. "Commercially reasonable methods" are often described as ones that rely on either government ID or "public or private transactional data". Two US states (Arkansas and Georgia) require the method to hold a NIST-approved Identity Assurance Level 2 (NIST, 2025[52]).

Jurisdictions that are listed as not specifying a particular method nonetheless usually require solutions to be feasible and proportionate. Three such jurisdictions (Czechia, Finland, and Slovenia) expressly prohibit the pre-checking of content, filtering, or preliminary control measures. Greece's law provides for the regulator to establish guidance on age verification, but this does not appear to have emerged yet.

Two OECD Member countries (Ireland and the United Kingdom) expressly provide that self-declaration should not be considered effective age assurance. The United Kingdom's Guidance relies largely on setting out principles for what underlies "highly effective age assurance" (i.e. technically accurate, robust, reliable, and fair), but also lists examples of what would and would not be considered highly effective age assurance.

Many of the above laws include a provision prohibiting any personal data collected for the purpose of assuring age from also being used for commercial purposes. Seven (Belgium, Czechia, Greece, Ireland, Iceland, Slovak Republic and Spain) limit this protection to children's personal data, reflecting requirements in the AVMSD. Nineteen apply this protection generally to any personal data collected for the purpose of assuring age (Alabama, Florida, Georgia, Idaho, Indiana, Kansas, Kentucky, Louisiana, Mississippi, Montana, Nebraska, North Carolina, Oklahoma, Slovenia, South Carolina, Sweden, Tennessee, Utah and Wyoming).

Age assurance requirements for the online purchase of age-restricted goods

As e-commerce has expanded, so has the online sale of age-restricted goods. To address the risk that children may be able to easily buy these goods online in some places, law makers have introduced requirements that retailers only allow access to their website once a user has verified their age (e.g. by

© OECD 2025

entering a date of birth)[14], or (either through laws or policy guidance) have made it clear that a physical ID check is required on delivery[15]. For some products, such as cigarettes, laws may prohibit online sales altogether[16].

Nonetheless, purchases of these goods online by children still occur and can have devastating consequences. For instance, a proposed law in the United Kingdom responds to a tragic incident where a 16 year old boy was murdered by other teenagers who had been able to purchase many of the knives used in the attack online without age assurance (Government of the United Kingdom, 2025[53]). Lawmakers have raised concerns that e-cigarettes in particular, which often come in flavours that might be appealing to children, are easily accessible to children (United States Congress, 2020[54]) (United Kingdom Parliament, 2024[55]), and there is evidence that children have indeed been able to easily purchase tobacco products including e-cigarettes online (Public Health Law Centre at Mitchell Hamline School of Law, 2022[56]). There is likewise evidence that online alcohol sales often occur without any ID check on delivery, even when there is a law in place requiring such a physical ID check (Alcohol and Drug Foundation, 2024[57]). A number of governments are considering introducing online age assurance mechanisms or requiring digital ID for the online purchase of age-restricted goods (Biometric Update, 2025[58]).

Accordingly, this section considers the current situation regarding laws relevant to the online sales of age-restricted goods. Taking the three examples of alcohol, cigarettes and knives, the section outlines where laws are in place that require an online age assurance process for the sale of these goods and how any such requirements are described in law[17]. The relevant laws relied on in this section are contained in Annex E.

Alcohol laws

While all countries analysed have laws prohibiting the sale of alcohol to children and young people (ranging from ages 16 to 20), safeguards regarding their online sale and subsequent delivery are rare.

- Two countries (Korea and Latvia) have a requirement for an online age assurance process. Latvia's law refers to age being verified via "qualified means of electronic verification". This online age assurance is only required when there is no "natural person" intermediary delivering the alcohol who can check physically check ID. Korea's law provides a list of acceptable age assurance methods.
- Eight countries (Czechia, Estonia, Finland, Germany, Iceland, Ireland, the Netherlands and the United Kingdom) all explicitly allow online sales and positively require an ID check at point of delivery. One country (New Zealand) allows online sales but is silent on the need for an ID check at point of delivery.
- Two countries (Switzerland and Türkiye) expressly prohibit online sales.
- Twelve countries (Chile, Colombia, Denmark, France, Hungary, Israel, Italy, Japan, Poland, Portugal, Slovak Republic, and Slovenia) positively require an ID check for the sale of alcohol, but do not mention the possibility of online sales.
- Ten countries (Belgium, Costa Rica, Germany, Greece, Lithuania, Luxembourg, Mexico, Norway, Spain, and Sweden) prohibit the sale of alcohol to children, but do not deal with online sales or delivery and do specify any obligation to verify age for this purpose.

Cigarette laws

Again, all countries analysed have laws prohibiting the sale of cigarettes (and often e-cigarettes) to children and young people (ranging from ages 16 to 20). The situation for cigarettes is more protective than for alcohol, with more countries both prohibiting online sales altogether or requiring online age assurance.

© OECD 2025

- Five countries (Czechia, Netherlands, Slovak Republic, Sweden and the United Kingdom) allow the online sale of cigarettes and establish an online age assurance requirement for this purpose.
- Twelve countries (Austria, Costa Rica, Estonia, Finland, Latvia, Lithuania, Mexico, Poland, Portugal, Slovenia, Spain, and Türkiye) expressly prohibit the online sale of cigarettes altogether.
- Korea and Germany both prohibit distance sales to children. Germany's law requires "technical or other precautions" be taken to prevent the delivery of cigarettes to children. Korea requires age assurance at point of sale, but it is not clear if this acts to prohibits online sales altogether or to establish a need to assure age for online sales. Similarly, the United States does permit the online sale of cigarettes and requires age assurance, but it is not clear if age assurance is to occur at point of sale or delivery.
- Twelve countries (Belgium, Chile, Colombia Denmark, France, Hungary, Iceland, Ireland, Israel, Italy, Japan, and Norway) positively require an ID check for the sale of cigarettes, but do not mention the possibility of online sales in their laws.
- Three countries (Greece, Luxembourg, Switzerland) prohibit the sale of cigarettes to children, but do not deal with online sales or delivery and do specify any obligation to verify age for this purpose.
- Eleven countries expressly cover the sale of e-cigarettes in their laws (Israel, Italy, Latvia, Netherlands, New Zealand, Poland, Portugal, Slovak Republic, Slovenia, Sweden, and Switzerland).

For those countries with laws that do specify an age assurance requirement, there is little guidance on how age assurance should actually occur.

- Czechia requires that the seller be equipped with a system that electronically verifies the consumers age via remote communication and requires information not just on age but also that the seller collect the customer's name and address.
- For three countries (the Netherlands, Slovak Republic and Sweden) the age assurance requirement is not accompanied by any further information as to how to meet this requirement. In the Slovak Republic however, the seller is required to give the administrative body detailed information on the age assurance system it uses.
- In the United Kingdom an "age verification system" is defined as "a computing system that confirms the consumer's age electronically".

Knife laws

The situation for the online sale of knives is much less protective than for either cigarettes or alcohol. While, as noted above the United Kingdom is in the process of developing a law that will aim to prevent children being able to purchase knives online (Government of the United Kingdom, 2025[53]) at present there is very few laws in place that deal with the sale of knives to children in general, or specifically online.

None of the countries analysed have an online age assurance requirement for the sale of knives, although one (Korea) does prohibit sales over the Internet. The United Kingdom, as part of its existing regime, operates a voluntary regime with major retailers that ID will be sighted on delivery. Requirements to obtain a permit to purchase a knife provides protection in some jurisdictions (Estonia, Japan, Lithuania, Luxembourg, Netherlands, Portugal and Slovenia), although it is not always clear which categories of knives (e.g. type, level of risk) this applies to. Poland allows online sales and is a country that requires a permit to purchase weapons however on the face of the law it is not clear that this applies to knives.

© OECD 2025

The laws do not always expressly prohibit the sale of knives to children, or deal with online sales. However, Korea does prohibit both sales to children and online sales. Belgium's law does not deal with sales to children but does prohibit online sales. Five countries (Austria, Costa Rica, France, Germany and Israel) prohibit sales to children but do not deal with online sales in their laws nor deal with a need to assure age. Some countries (Canada, Finland, and Switzerland) ban outright the sale or possession of certain types of dangerous knives.

The role of age rating schemes

Hard age limits also apply to games and media content (i.e. television and movies). These age limits are often found in classification (or content rating) schemes, which act to provide guidance on the content of the game or media itself and the appropriate age for viewing it or playing it. For instance, a classification scheme will provide guidance on the level of violence, nudity, coarse language in a piece of media and its consequent suitability for audiences of different ages (e.g. all ages, 7+, 12+, 15+ or 18+).

Classifications schemes are long standing. For instance, the Australian Classification Board has been in existence since 1917 (Parliament of Australia, 2025[59]), the United Kingdom's Game Rating Authority was initially established in 1989 (Games Rating Authority, 2024[60]) and the Entertainment Software Rating Board (ESRB) (which rates video games in the United States) in 1994 (ESRB, 2025[61]). While the ESRB has almost since its inception been concerned with online content[18], classification schemes were originally established to deal with fixed content. That is, a movie never changes no matter how many times you watch it; a "static" video game will always have the same game play or levels no matter how long it takes to get through it or how many different pathways a player can take to get to the end.

Today however, while classification schemes still act to provide ratings to movies, televisions shows and static video games whether they are served online or not, these systems also provide guidance (sometimes enforceable and sometimes not) on other online content. Most significantly on apps, or online video games that have user created spaces (and so are not static) and/or those that allow multiple online players, chat functions, and integrated purchases. While separate classification schemes may operate for "movies / television" and "video games", in both of the circumstances described here it is usually video game classification schemes that are used. As apps or online video games are likely to present the most risk to children, it is these schemes that are considered in this subsection.

Two major classification schemes operate that serve to generate most age ratings guidance globally for both video games and apps. These are the Pan European Game Information (PEGI) (PEGI, 2017[62]) age rating system which operates across Europe, and the Entertainment Software Rating Board (ESRB) in the United States and Canada (ESRB, 2025[63]). These rating systems are particularly ubiquitous across services used by children due to their use to classify apps in most apps stores other than the Apple App store. Apple runs its own system for generating age ratings for the apps on its service. This means that these ratings systems are used not just to classify games, but a large cross section of apps. Ranging from those that are indeed games, to social media, chat services, dating or AI apps, to mundane apps such as those used for banking or personal organisation. Apple, through its own classification system, also plays a significant role in generating age ratings for apps.

For apps and online games both PEGI and the ESRB use the International Age Rating Coalition (IARC) to generate an age rating (ESRB, 2024[64]) (PEGI, 2017[65]). The IARC age classification system offers game developers the ability to acquire an age rating for different classification schemes across the globe (IARC, 2024[66]). This includes PEGI and ESRB, but also certain government schemes including from Australia (Government of Australia, 2025[67]), Germany (USK, 2025[68]), and Korea (Game Rating and Administration Committee, 2025[69]). The IARC delivers a questionnaire and uses the answers to generate a rating that accords with the different schemes, which are then displayed in the different store fronts that use the IARC[19]. For those jurisdictions that are not covered by a participating age rating scheme the questionnaire

© OECD 2025

will generate a generic IARC rating. The different participating authorities are responsible for monitoring that ratings are accurate in their region (IARC, 2025[70]). Apple, for its part likewise generates a rating based on a questionnaire that it delivers to app developers (Apple, 2024[71]).

Neither the IARC nor Apple provide public versions of their questionnaires, but they do state publicly the types of questions developers are asked. Questions cover aspects related to content (e.g. violence, nudity) and in-app features (e.g. in-app purchases, unrestricted web access) (Apple, 2024[71]) (IARC, 2025[70]). The rating subsequently displayed in an app store or online video game store front is based on answers relevant to the content, and further information may be displayed on the interactive features available in the app or game. For services that have user generated content, an age rating scheme may provide statements on what the service itself says in its policy is about acceptable content and content moderation processes to inform on what content is likely to be on a service[20]. Apple's ratings are subject to manual review, and the company notes that due to the requirements of law in Australia, Brazil, France and Korea (Apple, 2024[72]) the App Store also displays regional age ratings in those countries. The IARC notes that each participating authority is responsible for monitoring ratings for accuracy in their region (IARC, 2025[70]).

The enforceability of classification schemes is dependent on the jurisdiction in which they operate as well whether the rating applies to an online or an offline game. For example, the United Kingdom's Video Recordings Act makes it illegal to supply a PEGI 12, 16 or 18 rated games to a person under those ages, however this does not apply online (Games Rating Authority, 2024[73]). Game publishers using the PEGI system commit to a Code of Conduct, which includes standards for safe online play (PEGI, 2017[74]). The ESRB system operates through the voluntary enforcement of retailers (both physical and online) who often require a game to have an ESRB rating before they will offer it for sale. Retailers then implement their own store policies to enforce age limits at point of sale, as well as being subject to ESRB mystery shop audits (ESRB, 2024[64]).

Classification schemes are an important part of the age assurance puzzle because they offer guidance that is then used by many popular apps and games. Regardless of the enforceability of guidance, parents or children themselves may rely on this guidance to decide whether to use an app or allow their child too. A product of the operation of different schemes, in conjunction with information on the minimum ages that services themselves set, can present a confusing picture. Notably, a service may set a different minimum age to what is recommended by Apple or through an IARC storefront (OECD, 2025[10]) .

Additionally, the provenance of the questionnaires that these schemes rely heavily on, and which operate via self-report from game developers, is opaque. A study considering Apple's system found no information on whether child development experts were involved in the design of the questionnaire, and it is not clear what decision making process is applied in translating the answers to the questionnaires into a rating (Canadian Centre for Child Protection, 2022[75]). There is evidence that apps or games may have a misleading age rating relevant to the risk they pose. For instance, 2024 research considering the apps on the Apple App Store found that out of 800 apps examined, more than 200 of those rated as appropriate for children as young as 4, 9, or 12, had concerning content or features. While in some categories, like stranger chat apps and games, most apps were rated 17+, in other categories like weight loss apps and unfiltered internet access apps, nearly all apps reviewed were approved for children 4+ (Heat Initiative[76]). This research noted that the Apple system would benefit from third party review, a transparent rating process based on expert guidelines on developmental appropriateness, and accountability and enforcement of age ratings (Heat Initiative, 2024[76]).

Brief conclusions

This section has considered the operation of laws and policies to enforce or provide guidance on hard age limits across three different areas. Laws aimed at preventing children accessing pornography are by far

© OECD 2025

the most protective, though clear gaps remain. The rules surrounding the purchase of age-restricted goods are uneven. Classification schemes, while commonly used to provide guidance on suitable ages for online services, appear lacking in terms of transparency, accountability and enforceability.

While all OECD Member countries prohibit children from being given access to pornography, there is distinct variation in the way this is enforced and applied to online distribution. Fifteen OECD Member countries do not address the online aspects of pornography distribution in their laws, and seven that do, do not require age assurance.

Laws that do contemplate age assurance are either very new (like the state-level laws in the United States) or largely arise from the AVMSD. It remains to be seen how the new laws will work in practice and how effectively they will be enforced, particularly considering that several rely on individuals bringing private claims and are not under the oversight of a regulatory authority. Meanwhile, the lack of specificity as to how to enforce the age verification requirement in the AVMSD, which has existed since 2018, has meant that many providers of online pornography rely on self-declaration, which is easily circumvented (Smirnova, Livingstone and Stoilova, 2021[7]).

Nonetheless, there is now a clear legislative focus on implementing age assurance solutions for pornography to effectively prevent a child's access. Several of the laws that set out more specifically how age assurance is to be carried out are very recent (e.g. Ireland's and the United Kingdom's) and are part of a wider online safety push. The move by a number of OECD Member countries to elaborate detailed guidance on age assurance shows both the momentum for greater online safety generally and a desire to get age assurance right.

Laws surrounding the online sales of age-restricted good are less protective, and the review of the laws aimed at preventing such sales demonstrates that concerns that children may be able to easily access such goods via online sales are reasonably well founded. Of the three case studies analysed, cigarettes have the most robust protections which are largely attributed to prohibitions on their online sale rather than to laws containing requirements for robust age assurance at the point of sale. None of the laws analysed establish age assurance requirements for the online sale of knives, and where such a requirement does exist for cigarettes or alcohol there is rarely specificity on how to meet the requirement.

Finally, classification schemes play a significant role in giving guidance on the age suitability of a wide variety of online apps and games with which children interact. However, these systems have evolved from providing guidance on fixed media content to covering wide-ranging services with dynamic and user-generated content, as well as a variety of potentially harmful functionalities. There is clear scope for policymakers to further consider the role these schemes play, their efficacy, as well as their transparency, accountability and (provided they are operating well) enforceability.

© OECD 2025

5 Privacy and data protection legal frameworks

This section considers age limits in privacy and data protection laws, and the extent to which they trigger protections for children. It also sets out where there are specific age assurance requirements in these laws, and where there has been specific action on behalf of privacy enforcement authorities related to age assurance in the form of policy guidance or a technical solution.

What are the relevant laws and age limits?

All OECD Member countries have established privacy and data protection regimes, and all but five have child-specific protections that give children's data special protections. Table 5.1 sets out which OECD Member countries: i) provide special protection for children's data and the relevant age for triggering these protections; ii) set an age limit for capacity to consent to data processing and the relevant age for triggering these protections; and iii) do neither.

Table 5.1. Age-related provisions in privacy and data protection laws

Jurisdiction	Provisions regarding special protection of children's data	Provisions regarding children's capacity to consent	No provisions regarding protection of children's data or capacity to consent	Relevant age for consent
Australia		•		Individual capacity, suggested threshold of 15
Austria	•	•		14
Belgium	•	•		13
Canada		•		Individual capacity, suggested threshold of 13
Chile			•	N/a
Colombia	•	•		18
Costa Rica		•		No set age
Czechia	•	•		15
Denmark	•	•		13
Estonia	•	•		13
Finland	•	•		13
France	•	•		15 (joint child/parental consent)
Germany	•	•		16
Greece	•	•		15
Hungary	•	•		16
Iceland	•	•		13
Ireland	•	•		16

© OECD 2025

Italy	•	•		14
Israel			•	18
Japan			•	No set age, suggested threshold of 13 or 16
Korea		•		14
Latvia	•	•		13
Lithuania	•	•		14
Luxembourg	•	•		16
Mexico			•	18
Netherlands	•	•		16
New Zealand		•		No set age
Norway	•	•		13
Poland	•	•		16
Portugal	•	•		13
Slovak Republic	•	•		16
Slovenia	•	•		15
Spain	•	•		14
Sweden	•	•		13
Switzerland			•	N/a
Türkiye		•		No set age
United Kingdom	•	•		13
United States	•	•		13

Source: Table A D.1. Age-based protections and methods for enforcing them in privacy and data protection laws.

Twenty-seven OECD Member countries require that children's data be treated with special protection, and impliedly require that a digital service provider know which of their users are children in order to implement this requirement. These are Colombia, the United States, all EU/EEA countries and the United Kingdom (which is bound by this requirement in the UK GDPR[21]). In all cases this age limit is 18, except in the United States where it is 13. The United Kingdom, through its Children's Code (United Kingdom Information Commissioners Office, 2020[77]), sets specific guidance on the appropriate protections for different age cohorts.

Two OECD Member countries (Canada and Türkiye) have guidance specific to the treatment of children's personal data, but their legal frameworks do not explicitly include these requirements so they are not listed in the first column in the table above.

Thirty-three OECD Member countries require that, if a child's data is processed on the basis of consent, then a parent must consent on their behalf. To effectively implement this requirement, digital service providers must be aware of their users' ages. Again, all EU/EEA countries and the United Kingdom have this requirement due to its inclusion in the GDPR[22]. Additionally, Australia, Canada, New Zealand, Türkiye and the United States have a consent requirement.

Across OECD Member countries there are a number of variations in the age limit set for consent, and the manner in which it is set:

- Eleven set this limit at 13, and a further two (Canada[23] and Japan) recommend 13 as the age at which a child would likely have this capacity but note this is to be determined on an individual basis (Japan also notes in some circumstances the appropriate threshold age may be 16).
- Five set the age limit at 14[24].
- Four set the age limit at 15. One (France) notes that consent is to be provided jointly between the parent and the child. Another (Australia) recommends 15 as the age at which a child would likely have this capacity but notes this is to be determined on an individual basis. Like France's,

© OECD 2025

Australia's law states that the consent should be actioned as far as practicable with the involvement of the subject of the consent.

- Seven set the age limit at 16.
- Three set the age limit at 18. Two of these (Israel and Mexico) do so as a result of provisions of other laws relating to the rights of children or citizens generally, and so this requirement is not obvious on the face of their privacy and data protection law.
- Three do not set a specific age limit, but their laws do refer to a need for capacity to consent or allow for a representative to consent on a person's behalf.
- Across EU/EEA countries and the United Kingdom, even though the consent requirement arises from the GDPR there is no uniformity in the age limit. This is because the GDPR provides that countries can set an age limit between 13-16 years. Ten of these countries set the limit at 13, four each set it at 14 and 15, and seven set it at 16.

Some OECD Member countries that require parental consent provide guidance on obtaining it with language like "reasonable efforts" or "considering available technology". In some cases, such as in France, Ireland, the Netherlands, and the United Kingdom, specific guidance accompanies the law, which provides detailed information on safeguarding children's privacy including on obtaining parental consent. In these cases, the guidance on parental consent is mostly limited to setting out principles related to proportionality, data minimisation, robustness, usability and compliance with industry or technical standards. Only Korea and the United States specify actual mechanisms for obtaining parental consent, including methods such as credit card authentication, email or text confirmation, or returning a consent form.

In addition to the protections set out above, some of the laws set out specific consumer-related protections relevant to the use of children's data, specifically prohibiting the use of such data for the purpose of behavioural or targeted advertising. These provisions are set out in Table 5.2.

Table 5.2. Age-related protections for targeted advertising

Jurisdiction	Details of provision	Age limit
EU countries	The Digital Services Act (2022) requires that online platforms cannot present personalised advertisements based on profiling using the personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a child.	18
France	In addition to EU requirements, guidance from the privacy enforcement authority (the CNIL) states that children's data cannot be reused or transmitted to third parties for the purpose of advertising, unless it can be demonstrated that this is for a compelling reason.	18
Ireland	In addition to EU requirements, guidance from the privacy enforcement authority (the DPC) specifies that online service providers should not profile children and/ or carry out automated decision making, or otherwise use their personal data for marketing/ advertising purposes unless they can clearly demonstrate how and why it is in the best interests of the child to do so.	18
Korea	Guidance from the privacy enforcement authority (the PIPC) sets out that if online service providers intend to combine children's behavioral data with their unique identification information for the purpose of targeted advertising, they must obtain consent. Even with consent, it is recommended that online services minimise targeted advertising, and do not collect or use children's behavioural data for this purpose.	14
United Kingdom	The ICO's age-appropriate design code requires that unless there is a compelling reason otherwise, options within a service that rely on profiling must be switched off by default. Guidance within the Children's Code notes that the use of non-essential cookies for behavioural advertising can only be permitted on the basis of consent.	18
United States	The COPPA Rule provides that any data collected for supporting a website or online services internal operations, cannot be used to "contact a specific individual, including through behavioral advertising".	13

Source: Table A D.1. Age-based protections and methods for enforcing them in privacy and data protection laws.

© OECD 2025

While all the protections in the laws and guidance in the table above can likely be achieved through compliance with the broader child-specific protections in the privacy and data protection laws, they nonetheless add to a fragmented landscape. These laws have varied threshold ages, with some allowing profiling for targeted advertisement on the basis of consent and some being silent on this aspect, and still others setting out that profiling for this purpose may be permissible if a best interests criterion can be demonstrated.

Finally, legislative action aimed at strengthening protections for children's data is underway in several OECD Member countries. Australia passed a law in December 2024 proposing a comprehensive Children's Online Privacy Code. That Code, which is in now (as of March 2025) the process of being developed, is anticipated to be in place by December 2026 (Office of the Australian Information Commissioner, 2025[78]). Colombia introduced a bill in 2021 to strengthen children's privacy rights (Government of Colombia, 2021[79]), and Costa Rica proposed comprehensive privacy reform in the same year (Government of Costa Rica[80]). Additionally, the United Kingdom is considering a bill that includes several measures aimed at enhancing children's protections (United Kingdom Parliament, 2025[81]).

What are the age assurance requirements?

As seen above, most OECD jurisdictions have protections in their privacy laws that imply a need to assure age, but there are significantly fewer express age assurance requirements in these laws. Those that do exist are set out in Table 5.3, which specifies whether a country's age assurance requirement is in a law or in a guidance document, whether the guidance sets out specific age assurance mechanisms that could be applied (and what they are) and when the guidance is limited to stating underlying principles for age assurance.

Table 5.3. Age assurance methods for privacy and data protection mentioned in laws

Jurisdiction	Source	Self-declaration	Parent confirmation	3rd party service	User flags	Technical measures	Sets out principles
France	Guidance						•
Ireland	Guidance						•
Korea	Guidance	•			•	•	•
Netherlands	Guidance	•	•	•		•	•
Türkiye	Guidance	•				•	•
United Kingdom	Statutory Code						•

Source: Table A D.1. Age-based protections and methods for enforcing them in privacy and data protection laws.

In the domain of privacy and data protection, most jurisdictions provide direction on appropriate age assurance via guidance documents, save for the United Kingdom whose guidance is set out in a statutory code. For those that set out principles, the principles generally require that age assurance be:

- proportionate to risk
- robust and effective
- reliable
- technically accurate
- simple and easy to use

© OECD 2025

- be operated in a fair manner
- comply with any industry standards, and
- be privacy protective and minimise data collection.

In two countries (Korea and the Netherlands), the principles elaborated are limited to the need to minimise data collection. In the Netherlands, use of self-declaration is specified as being applicable only to low-risk situations.

In addition to setting out guidance relevant to enforcing the privacy and data protection laws in their jurisdictions, a number of privacy enforcement authorities provide specific guidance relevant to the privacy implications of a wider rollout of age assurance in their jurisdiction (i.e. also to meet an online safety requirement). These either set out more detailed principle-based guidance, accepted technical standards, or elaborate their own proposed solution. These are set out in Table 5.4.

Table 5.4. Age assurance guidance elaborated by privacy enforcement authorities

Authority	Principles	Technical standards	Technical solution
OPC, Canada	• (Consultation stage)		
CNIL, France	•		•
AEPD, Spain	•		
AEPD, Spain		•	
ICO, UK	•		

Source: (Commission Nationale de l'Informatique et des Libertés, 2022[82]) (Commission Nationale de l'Informatique et des Libertés, 2022[83]) (Agencia Española de Protección de Datos, 2023[84]) (Agencia Española de Protección de Datos, 2023[85]) (Canada Office of the Privacy Commissioner, 2024[86]; Agencia Española de Protección de Datos, 2024[87]) (United Kingdom Information Commissioners Office, 2024[88]).

In addition to the above, in February 2025 the European Data Protection Board (EDPB) issued a statement on age assurance that lists ten principles for the compliant processing of data for the purpose of age assurance. These principles include that GDPR-compliant age assurance processes should be rights based, proportional to risk, not lead to any unnecessary data protection risks, respect data minimisation and purpose limitation principles, be effective, lawful, fair and transparent, protect data by design and default, be secure and be accountable (European Data Protection Board, 2025[89]).

Brief conclusions

Most but not all OECD Member countries have provisions in their privacy and data protection laws that imply a need to know whether a user is a child for the purpose of applying statutory protections. These protections vary in both their purpose and the age threshold at which they apply.

When the protection is relevant to giving children's data special protection (including for the purpose of targeted advertisements), the age limit is for the most part uniformly set at 18, though in one case it is 13. While some jurisdictions set out guidance for assuring age, only one jurisdiction (the United Kingdom) has an enforceable framework, and the framework recognises that the necessary protections for children may differ depending on their age and stage of development.

The requirements implying a need to be aware of a user's age for the purpose of obtaining parental consent likewise vary. The threshold age differs across jurisdictions and is set between the ages of 13 and 18, with five jurisdictions not addressing the need for parental consent at all and two providing that a determination of capacity to consent needs to be made on a case-by-case basis. Unlike blanket requirements to provide children's data with special protection, consent requirements will not be engaged every time a child's data

© OECD 2025

needs to be processed, but rather only when the legal basis underlying that processing is consent (as opposed to processing on another legal basis, such as legitimate interest).

Privacy enforcement authorities are also turning their minds towards the privacy and data protection implications of age assurance for purposes beyond enforcing laws under their responsibility. Several have elaborated principles, standards, or their own technical solution for assuring age in a privacy preserving way that they recommend be applied when age assurance is required for any reason (e.g. for an online safety purpose).

© OECD 2025

6 Conclusion

The legal landscape for age assurance is complex. Age limits exist for a variety of reasons and the manner of their enforcement varies. This is true across both legal disciplines (e.g. safety and privacy) and borders.

For the most part, age assurance requirements are implied, arising because a service needs to know which users are children to implement a specific protection appropriately. Even where the requirement is express, there is ambiguity. No law sets out one specific age assurance method that must be applied and only those laws relevant to pornography and Korea's online safety law tend to establish an age assurance requirement that cannot be abated by taking some other action. A few laws dealing with the sale of online goods contain an express requirement to assure age online, but they are sparse and lack specificity on how to operationalise them. Classification schemes that provide guidance on recommended age ratings do not necessarily involve child development experts in their processes, rely heavily on self-reporting from the developers of online services, and often lack transparency, accountability and enforcement mechanisms.

Privacy is an important thread running through all aspects of age assurance, and not only for respecting age limits or age-based protections in privacy and data protection laws. Several safety-based age assurance requirements explicitly include provisions relevant to ensuring that any data collected for the purpose of assuring age is not retained or used commercially. Interestingly, however, in many cases this protection is limited to children's data whereas the requirement to assure age applies to the whole audience seeking access to a site. Privacy regulators are clearly attuned to the importance of protecting data that is collected for the purpose of assuring age and are driving many regulatory activities aimed at delivering good age assurance solutions.

Nonetheless, despite the underlying importance of privacy in age assurance, the current push to better legislate for age assurance derives from concern for children's safety. The safety landscape, though, is also complex. Other than in laws regulating access to pornography, in which the age limit across the OECD is almost uniformly set at 18 and the regulated content is of a static type, safety age limits and consequent age assurance provisions are varied. Sometimes online safety laws apply only to social media; in other cases, they relate to online harms more broadly, and in some cases, they apply specifically to online games. Regulated content is often described in imprecise terms without clearly specifying what is banned, and threshold ages vary. At the same time, new requirements are on the horizon in the form of proposed laws or pending guidance for implementing recently adopted laws. Co-operation between regulators is important to ensure cross-regulatory cohesion and such collaboration is already occurring in several jurisdictions.

There is, however, a clear trend of defining content children need protecting from, the vulnerabilities of different age cohorts, how age assurance can best be implemented, what underlying principles are important for age assurance approaches, and the responsibilities of digital service providers in implementing these requirements. This is key. Achieving effective age assurance which can ensure that services know which of their users are children is fundamental in providing a safe and beneficial digital environment for children.

© OECD 2025

Annex A. Laws and policies regulating online harms

Table A A.1 sets out laws and policies that address online harms and includes provisions on the protection of children that either expressly require age assurance or contain a measure that implicitly requires age assurance. OECD Member countries that do not have such a law or policy are not reflected in this table. Jurisdictions that have a proposed online safety law with these characteristics are noted.

The EU has two laws: the Digital Services Act (DSA) (European Commission, 2022[35]) and the Audiovisual Media Services Directive (AVMSD) (European Commission, 2018[34]). The DSA directly affects EU Member States, so unless the country has a standalone law addressing online safety, its provisions are not duplicated across EU Member States in this table. The AVMSD is the basis of many EU laws addressing pornography, and it has also been reflected in Table A C.1. Laws incorporating the AVMSD's requirements are reflected in this table when their provisions go beyond regulating access to pornography. For EU Member States, in most cases only the law fulfilling the AVMSD's mandate has been detailed, but under the column "Administrator" both the authorities responsible for administering the AVMSD and those that will be, or have been, designated as the Digital Service Coordinator under the DSA are listed.

As noted in Section 1, this research is concerned only with laws that require (expressly or impliedly) age assurance. Accordingly, some OECD Member countries that have laws covering online harms are not reflected in this table, as their laws do not have provisions relevant to age assurance.

Table A A.1. Age-based protections and age assurance requirements in online safety laws and policies

Country / Region	Law	Age limit	Purpose / Scope of law	Online age assurance requirement	Administrator
Australia	Online Safety Act (Government of Australia, 2021[90])	**16/18**	Australia's Online Safety Act sets out measures that implicitly require age assurance in two ways: Basic Online Safety Expectations (BOSE) (s 46) The BOSE require *inter alia* that service providers "take reasonable steps to ensure that technological or other	The Act does not set out any express age assurance requirement. In the Class 1 codes and standards there is no current online age assurance requirement, other than that set out in the Social Media Code (see Table A B.1). The eSafety Commissioner is currently running an age assurance trial to test the efficacy of age verification and age estimation technologies	eSafety Commissioner

© OECD 2025

Country / Region	Law	Age limit	Purpose / Scope of law	Online age assurance requirement	Administrator
			measures are in effect to prevent access by children to class 2 material provided on the service" (at art 46(d)). (See definition of class 2 below). Industry Codes & Standards (Division 7) The Act provides for the development of Industry Codes and Standards which set out enforceable measures for industry in complying with the objectives of the Act. Industry Codes are co-designed between the Commissioner and industry representatives. Industry Standards are drawn up by the Commissioner when agreement on a Code has not been reached. There are currently six codes in place addressed at: social media services, app distribution services, hosting services, internet carriage services, equipment providers, and search engine services; and two standards in place, addressed at: electronic services and designated internet services. The codes in place deal with class 1 material (Australia's eSafety Commissioner, 2024[91]). As of March 2025, codes to deal with class 2 material, are under development, and are at consultation stage (Australia's eSafety Commissioner, 2024[38]) (Online Safety Australia, 2025[39]) (see definitions of class 1 & 2 material below). At present these draft codes envisage age assurance requirements for dating and gaming services, and to prevent access to self-harm material (and pornography) (Online Safety Australia, 2025[39]). For services that i) enable end users to search for or communicate with other end-users; ii) are interactive gaming services; and iii) are high risk, the **Relevant Electronic Services (RES) Standard** has the following requirements which imply knowledge of the end-users age: • setting the account of a young Australian child at private by default;	in protecting children from encountering *inter alia* online pornography (Australia's eSafety Commissioner, 2024[48]) (Age Assurance Technology Trial, 2025[47]). At the same time, the Commissioner is developing industry codes that will regulate Class 2 material (Australia's eSafety Commissioner, 2024[38]) (Online Safety Australia, 2025[39]). Guidance from the eSafety Commissioner notes that while the trial will not specifically inform the creation of the codes, consideration will be given to how outputs from the trial can inform and support the development of the codes. Adding context not only to "what industry is expected to do (e.g., take reasonable and appropriate steps to confirm users' age) and when or where they should do it" but also guidance on "the how (e.g., by informing what reasonable and appropriate steps for compliance may be best within the Australian context)" (Australia's eSafety Commissioner, 2024[38]). The current consultation drafts of the phase 2 codes refer to age assurance measures needing to be "technically feasible and reasonably practicable" (Online Safety Australia, 2025[39])	

© OECD 2025

Country / Region	Law	Age limit	Purpose / Scope of law	Online age assurance requirement	Administrator
			• not allowing end-users know the location of a young Australian child end-user, without the consent of the child's parent or carer. High risk designated internet services (see Part 3 of the Standard) must: • ensure that a child in Australia who is known by the provider to be under the age of 18 does not become an end-user of the service; and • stop access to the service by a child in Australia who is known by the provider to be under the age of 18. Definitions **Australian child** is an Australian end-user under the age of 18 years. **Young Australian child** is an Australian end-user under the age of 16 years. **Class 1A** material is illegal content, including child sexual exploitation and abuse material and terrorist and violent extremist content (see s106, and (Australia's eSafety Commissioner, 2023[92]) **Class 1B** material is crime or violence material, or drug related material (see s106, and (Australia's eSafety Commissioner, 2023[92]) **Class 1C** material is online pornography that describes or depicts specific fetish practices or fantasies (see s106, and (Australia's eSafety Commissioner, 2023[92]) **Class 2A** material is other online pornography that depicts actual (not simulated) sex between consenting adults**.** (see s106, and (Australia's eSafety Commissioner, 2023[92]) **Class 2B** material is: • online pornography, which includes realistically		

© OECD 2025

Country / Region	Law	Age limit	Purpose / Scope of law	Online age assurance requirement	Administrator
			simulated sexual activity between adults, and which includes high-impact nudity; and • other high-impact material which includes high-impact sex, nudity, violence, drug use, language and themes (i.e. crime, suicide, drug and alcohol dependency, death, serious illness, family breakdown and racism). (see s106, and (Australia's eSafety Commissioner, 2023[92])		
Austria*	Audiovisuelle Mediendienste-Gesetz (AMD-G) (Federal Act on Audiovisual Media Services) (Government of Austria, 2020[93])	**18**	*Act transposes the AVMSD.* The law provides that content in audiovisual media services that may impair the physical, mental or moral development of minors may only be provided by the media service provider in such a way that it cannot normally be perceived by minors (at s39). It further requires age assurance be used to prevent children gaining access to online depictions of **gratuitous violence** (at s54e). Gratuitous violence is not defined. While the AMD-G does not define "minor", the Austrian Civil Code defines a minor as a person not yet 18 years of age (at s21) (Government of Austria, 2018[94]).	The law does not prescribe any particular age assurance method.	KommAustria (**AVMSD & DSA**)
Belgium*	Loi relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale (Law relative to audiovisual media services in the bi-lingual region of Brussels Capital) (Government of Belgium, 2017[95])	**18**	*Act transposes the AVMSD.* The law provides that video-sharing platform service providers are to take appropriate measures to protect minors from "programmes, user-generated videos and audiovisual commercial communications that may be harmful to their physical, mental or moral development" and ensuring that such content is only made available under conditions that prevent minors from seeing or hearing it. **Gratuitous violence** (along with pornography) is considered the most harmful content (at art. 29/1). Appropriate measures include "setting up and using systems for verifying the age of users" (at art. 29/1, § 2 (3))	The law does not prescribe any particular age assurance method. The law does provide that any personal data from children collected or generated for the purpose of age verification cannot be processed for commercial purposes (at art. 29/1, § 2 (3)).	Institute for Postal Services and Telecommunications (BIPT) (**AVMSD & DSA**)

© OECD 2025

Country / Region	Law	Age limit	Purpose / Scope of law	Online age assurance requirement	Administrator
			Minor is not defined in the law however the Belgium Civil Code defines a minor as a person not yet 18 years of age (at s488) (Government of Belgium, 1804[96]).		
Czechia*	Zákon o službách platforem pro sdílení videonahrávek a o změně některých souvisejících zákonů (zákon o službách platforem pro sdílení videonahrávek (the Video Sharing Platform Services Act) (Government of Czechia, 2022[97])	**18**	*Act transposes the AVMSD.* The law provides that video-sharing platform service providers are to adopt measures to "protect minors from programmes, user-generated videos and commercial communications which might impair their physical, mental, or moral development", and that such content "are only made available in such a way as to ensure that minors will not normally hear or see them". The law further notes that "measures to protect minors include, in particular, age verification tools or other technical measures" (at § 7(1)). The law further provides that "the most objectionable content that may impair the physical, psychological or moral development of minors, such as pornography or **gross self-inflicted violence**, shall be subject to the strictest measures to control access" (at § 8(2)), which includes "age verification" (at § 8(3)(f)) (emphasis added). **Minor** is not defined in this law however Czechia's Civil Code defines them as individuals who have not yet reached 18 (at § 30) (Government of Czechia, 2012[98]). **Video sharing platform** is as defined in the AVMSD, however the law specifies that it applies to those established in Czechia (at §.3)	The law does not prescribe particular methods of age assurance but does note that in applying any of the "strictest measures" – which includes age verification – that the measure must be "feasible and proportionate to the scale and nature of the video-sharing platform service provided and shall not lead to filtering of uploaded content or to preliminary control measures" (at § 8(1)). The law further provides that any personal data from children collected for the purpose of establishing *inter alia* age assurance mechanisms, must not "be processed for commercial purposes, in particular, for direct marketing, profiling and behavioural advertising" (at § 9).	Český telekomunikační úřad (ČTÚ) (**DSA**) Rada pro rozhlasové a televizní vysílání (RRTV) (**AVMSD**)
Denmark*	Bekendtgørelse om videodelingsplatformstjeneste (Notice on Video Sharing Platform Services) (Government of	**18**	*Act transposes the AVMSD.* The law provides that video-sharing platform service providers are to "take appropriate measures to protect minors from programs, user-generated videos, advertising, sponsorship and product placement that may harm their physical, mental or moral development" (at § 11). Such	The law does not prescribe particular methods for "age control". It does note that any measures taken (included those for age control) must be "feasible and proportionate and take into account the size of the video sharing platform service and the nature of the service offered" (at §15). The law further provides that any personal data from children collected for the purpose of establishing *inter alia* age assurance mechanisms	Radio og tv-nævnet (Radio & Television Board) (**AVMSD**) Digitaliseringsstyrelsen (Agency for Digital Government

© OECD 2025

Country / Region	Law	Age limit	Purpose / Scope of law	Online age assurance requirement	Administrator
	Denmark, 2020[99])		measures include, "establishing and maintaining systems for age control of users of video-sharing platforms" (at §12(4)). The most harmful content is required to be subject to the "strictest control measures" (at §12, paragraph 2). Content that would cause such "**harm**" is not defined, nor is what would constitute the "**most harmful content**". **Minor** is not defined in the law, however Denmark's Guardianship Act provides that a person obtains majority from the age of 18 (at §1) (Government of Denmark, 2007[100]). **Video sharing platforms** are defined as per the AVMSD, however the law specifies that it applies to those established in Denmark (at §5).	"may not be processed for commercial purposes such as direct marketing, profiling and behavioral advertising" (at §12, paragraph 3). *See also Denmark's Ethical Guidelines (described in* Table A B.1*), which focus on social media but could also be applied to online harms more generally and provide age assurance guidance* (Danish Media Council for Children and Young People, 2025[101]).	(**DSA)**
Estonia*	Estonia's law transposing the AVMSD, when dealing with the activities of video sharing platforms and preventing children from accessing material that may harm their "physical, mental or moral development", largely prescribes measures amounting to prohibitions in terms of use or technical filtering. One provisions does call for providing content in a manner that "can only be received by means of personal identification codes or other appropriate technical solutions in a way that is normally inaccessible to a minor"(at § 19(5)), however it is not clear whether this would include age assurance technologies (Government of Estonia, 2010[102]).				Tarbijakaitse ja Tehnilise Järelevalve Amet (TTJA) (**AVMSD & DSA**)
European Union	*Audiovisual Media Services Directive (AVMSD)* (European Commission, 2018[34])	***18***	*Article 28b of the AVMSD provides that "Member States shall ensure that video-sharing platform providers under their jurisdiction take appropriate measures to protect (…) minors from programmes, user-generated videos and audiovisual commercial communications which may impair their physical, mental or moral development in accordance with Article 6a(1)"* *Article 6a (1) of the AVMSD requires "Member States to take* ***appropriate measures*** *to ensure that audiovisual media services provided by media service providers under their jurisdiction which may impair the physical, mental or moral development of minors are only made available in such a way as to ensure that minors will not normally hear or see them". The most harmful content, such as gratuitous violence (and pornography, addressed in* Table A C.1*) are*	*Article 28b specifies that the most harmful content shall be subject to the strictest access control measures. As appropriate, those measures inter alia include, "establishing and operating age verification systems for users of video-sharing platforms with respect to content which may impair the physical, mental or moral development of minors".* *Article 6a specifies that appropriate measures "may include selecting the time of the broadcast,* ***age verification tools*** *or other technical measures" (emphasis added)* *Any measures taken are to be proportionate to the potential harm. Any personal data of minors collected or otherwise generated by media service providers for the purpose of implementing appropriate measures are not to be processed for commercial purposes.*	*European Commission* *Member State supervisory authorities*

© OECD 2025

Country / Region	Law	Age limit	Purpose / Scope of law	Online age assurance requirement	Administrator
			to be subject to the strictest measures. *<u>Definitions:</u>* ***Minor** is not defined in the AVMSD, however the European Commission's Better Internet for Kids Policy defines children as individuals under 18 years* (European Commission, 2022[103]). ***Video-sharing platform** services are those "where the principal purpose of the service or of a dissociable section thereof or an essential functionality of the service is devoted to providing programmes, user-generated videos, or both, to the general public, for which the video-sharing platform provider does not have editorial responsibility, in order to inform, entertain or educate, by means of electronic communications networks (…) and the organisation of which is determined by the video-sharing platform provider, including by automatic means or algorithms in particular by displaying, tagging and sequencing".*		
European Union	*Digital Services Act (DSA) (2022)* (European Commission, 2022[35])	***18***	*Art 28 of the DSA requires that "providers of online platforms accessible to minors shall put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service".* *Recital 71 specifies that "an online platform can be considered to be accessible to minors when its terms and conditions permit minors to use the service, when its service is directed at or predominantly used by minors, or where the provider is otherwise aware that some of the recipients of its service are minors, for example because it already processes personal data of the recipients of its service revealing their age for other purposes".* *As of March 2025, the European Commissioner has not*	*The DSA does not specify any particular age assurance method for the purpose of art. 35; or if it is required in the application of art 28. Art 28 does further provide that providers of online platforms shall not be obliged to process additional personal data in order to assess whether the recipient of the service is a minor.* *In January 2024 DG-Connect established a task force on age verification, however (as of March 2025) no recommendations or guidance have been released by the taskforce* (European Commission, 2024[45]).	*European Commission* *Digital Service Coordinators*

© OECD 2025

Country / Region	Law	Age limit	Purpose / Scope of law	Online age assurance requirement	Administrator
			provided any implementation guidance for article 28, however such guidance is in development (European Commission, 2024[37]). *Additionally, article 35 of the DSA requires very large online platforms (VLOPs) and very large online search engines (VLOSEs) to put in place "reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks identified" in a mandated risk assessment (pursuant to Article 34). Such measures are to be applied with particular consideration to their impact on fundamental rights, and may include* inter alia *"taking targeted measures to protect the rights of the child, including age verification and parental control tools, tools aimed at helping minors signal abuse or obtain support, as appropriate"* *Definitions:* ***Minor** is not defined in the DSA, however the European Commission's Better Internet for Kids Policy defines children as individuals under 18 years* (European Commission, 2022[103]). ***Online platforms** are "a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation".* ***Online search engines** are "an intermediary service that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form*		

© OECD 2025

Country / Region	Law	Age limit	Purpose / Scope of law	Online age assurance requirement	Administrator
			of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found". ***VLOPs** and **VLOSEs** are online platforms or online search engines with average monthly active recipients in the EU of 45 million or more, and that are designated by the EU as a "VLOP" or "VLOSE".*		
Finland*	Kuvaohjelmalaki (Image Program Act) (Government of Finland, 2011[104])	**18**	*Act transposes the AVMSD.* The law provides that video sharing platforms "must take appropriate measures to protect children from such image programs that may be harmful to the child's development" (at s7A). Programs harmful to a child's development are those that due to "**violence** or sexual content, or **by causing anxiety**" can cause harm to a child's development. In evaluating harmfulness, consideration should be given to the context in which the content is presented (at s15) (emphasis added). **Minor** is not defined in the law, however Finland's Act on Guardianship defines a minor as persons under the age of 18 (at s2) (Government of Finland, 1999[105]).	The law does not expressly define "appropriate measures" to include age assurance. It does note that any measures must be "proportionate to the nature of the video programs in question and the potential harm caused by them, taking into account the size of the video sharing platform service and the nature of the service offered". And that "the measures must not lead to pre-checking of content or filtering applied to uploading to the platform" (at s7a).	Traficom (**AVMSD & DSA**)
France*	Léotard Loi (Government of France, 1986[106]) SREN Loi (Government of France, 2024[107]) Code Pénal (Government of France, 1810[108])	**18**	AVMSD The Léotard Law (which transposes the AVMSD) requires video sharing platforms to take appropriate measures to protect minors from programs, user-created videos, and audiovisual commercial communications that are likely to harm their physical, mental or moral development. It specifies that "appropriate measures" include implementing an age verification system (at art 60). However, it does not specify what kind of content would be harmful to minors. SREN Law The SREN Law establishes a three-year pilot regime on	Arcom adopted a framework on technical measures for age assurance specific to online pornography in October 2025 (Arcom, 2024[110]). See also Annex C. The Léotard Law specifies that the personal data of minors collected or generated by providers of video sharing platforms for the purpose of assuring age, must not be used for commercial purposes, even after the child has reached majority (at art 60).	Arcom (**AVMSD &DSA**)

© OECD 2025

Country / Region	Law	Age limit	Purpose / Scope of law	Online age assurance requirement	Administrator
			online games with monetisable digital objects – from the date of promulgation (May 2024). This regime includes a requirement that companies offering such games prevent minors from participating in a game for payment via AVMSD compliant age verification (at art. 41). Minor is not defined in the above two laws, however France's Civil Code establishes 18 as the age of majority (at art. 414) (Government of France, 1804[109]) <u>Criminal law</u> France's Penal Code prohibits "manufacturing, transporting, distributing by any means whatsoever and on any medium a message of a violent nature, inciting terrorism, pornographic, including pornographic images involving one or more animals, or likely to seriously undermine human dignity or to incite minors to engage in games that put them in physical danger, or of trading in such a message". It expressly provides that the offence will be constituted even if the minor's access resulted from a self-declaration indicating that they are at least 18 years old (at art. 227-24).		
Germany*	Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien (Jugendmedienschutz-Staatsvertrag – JMStV) (Government of Germany, 2002[111]) (Interstate Treaty	**18**	*Act transposes the AVMSD.* The Act requires video sharing providers to take "appropriate measures to protect children and young people from offers (of content) that are detrimental to their development" (at § 5a(1)). Establishing and operating an age verification system, amounts to an appropriate measure" (at § 5a(2)). The law defines a **child** as someone who is not yet 14, and a young person as someone between the age of 14 and 18 (at § 3 JMStV, § 1 JuSchG). The JuSchG does define which particular content would be detrimental to children's development, and this includes	The law does not prescribe any particular age assurance methods. However, KJM (Germany's Commission for Youth Media Protection) has issued guidance on age assurance, recommending that any system comprise both an identification component, and an authentication component (Kommission für Jugendmedienschutz, 2024[41]). On behalf of the Federal Ministry for Family Affairs, Senior Citizens, Women and Youth, the Fraunhofer Institute has developed a concept for data-saving age verification (Heise Online, 2025[114]) (Fraunhofer IDMT, 2025[115]).	Landesmedienanstalten, Kommission für Jugendmedienschutz (KJM) (**AVMSD)** Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA), and, for Art. 28 para. 1 of the DSA, Bundeszentrale für

© OECD 2025

Country / Region	Law	Age limit	Purpose / Scope of law	Online age assurance requirement	Administrator
	on the Protection of Minors in the Media) Jugendschutzgesetz (JuSchG) (Youth Protection Act) (Government of Germany, 2002[112])		content that is excessively frightening, advocates violence or impairs socio-ethical values (§§ 10b and 15 (1)). Additionally, the BzKJ provides guidance (Bundesprüfstelle für jugendgefährdende Medien, 2024[113]).		Kinder- und Jugendmedienschutz (BzKJ) (**DSA**) BzKJ **(JuSchG) and** Landesmedienanstalten
Greece*	Law 4779 of 2021 (Government of Greece, 2021[116])	**18**	*Act transposes the AVMSD.* The law states that video sharing platforms "must take appropriate measures to protect minors" from videos and programs that "may have a negative effect on their physical, mental or moral development" (at art 32(1)). The law specifies that for the purpose of protecting minors, "the most harmful content is subject to the strictest access control measures, which include the "installation and operation of systems for verifying the age of users of the platform, in order to prevent access by minors (at s32(6))". The "most harmful content" is defined as including "**gratuitous violence** and pornography" (at art. 9.1) (emphasis added). **Minor** is not defined in the law, however Greece's Civil Code (at art. 127) defines a minor as persons under the age of 18 (Government of Greece, 1946[117]). **Video sharing platform** is as defined in the AVMSD, however the law specifies that it applies to those established in Greece (at art. 31)	The law does not prescribe any particular age assurance methods. The law does provide that the ESR can establish guidance / procedures for complying with any of the "appropriate measures" (and so, including age assurance) (at art. 32.8); and that the ESR can ask video sharing platforms for information on *inter alia* age assurance systems (at art. 32.10). The law further provides that any personal data from children collected for the purpose of establishing *inter alia* age assurance mechanisms, must not be "subject to processing for commercial purposes" (at art. 32.7).	National Council for Radio & Television (ESR) (**AVMSD)** Hellenic Telecommunications and Post Commission (EETT) (**DSA)**
Hungary*	2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások,	**18**	*Act transposes the AVMSD.* The law provides that video sharing platforms are to apply measures and protections if *inter alia* the content is "capable of harming the physical, intellectual, spiritual or	The law specifies that age verification is required to comply with the requirement in s15/D. It is specified (as s 15/F) that: • to be considered effective the age verification method must prevent minors from seeing or hearing the harmful content; • the measure will be considered appropriate if it is proportionate to	Nemzeti Média- és Hírközlési Hatóság (NMHH) (**AVMSD & DSA**)

© OECD 2025

Country / Region	Law	Age limit	Purpose / Scope of law	Online age assurance requirement	Administrator
	valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről (Law on certain issues of electronic commercial services and services related to the information society) (Government of Hungary, 2001[118])		moral development of minors" (at s15/D). The law does not define what would amount to such harmful content, but does provide that age verification is an applicable measure. **Minors** are not defined in this law, but pursuant to the Civil Code are defined as persons under the age of 18 (at §2. (Government of Hungary, 2013[119]).	the disadvantage and damage caused by the content; It is further noted that age verification measures should not lead to preliminary control measures or filtering of content uploads; and that the personal data of minors collected or otherwise generated by the video sharing platform service provider for the purpose of age verification must not be processed for commercial purposes (at s 15/F). Hungary's Digital Child Protection Strategy (Government of Hungary, 2016[120]) does set out some suggestions for age assurance mechanisms, being: • use of a credit card or other payment method able to sufficiently demonstrate the card holder's age; • using reliable and authentic databases similar to the electoral register (noting potential data protection concerns with this suggestion); • demonstrating holding a mobile phone subscription only available for persons with ID; or • Using personal identification numbers. The strategy does recognise that such requirement would need to be established in law, which as of March 2025, has not occurred.	
Iceland*	Lög um fjölmiðla (Act on the Media) (Government of Iceland, 2011[121])	**18**	*Act transposes the AVMSD.* Video sharing platforms are required to "take appropriate measures to protect children from content, user-generated content and commercial messages that may harm their physical, mental or moral development" (at art 36.a). Such content is noted to be in particular "content that includes pornography or **gratuitous violence**" (at art. 28) (emphasis added). Such measures include establishing and operating "an age verification system" (at art 36.d.g). The law does not define a minor, however Iceland's Law of Jurisdiction, defines the age of majority as 18 (at art. 1)	The law does not prescribe any particular age assurance methods. The law does provide that any personal data from children collected for the purpose of establishing *inter alia* age assurance mechanisms, must not be used for commercial use (at art. 36).	Fjolmidlanefnd

© OECD 2025

Country / Region	Law	Age limit	Purpose / Scope of law	Online age assurance requirement	Administrator
			(Government of Iceland, 1997[122]).		
Ireland*	Online Safety and Media Regulation Act (Government of Ireland, 2022[123])	**18**	Ireland's Act, both transposes the AVMSD and establishes a broader online safety regulatory regime. The Act provides for the CnaM to make an Online Safety Code and designate online service providers (including video-service providers under Ireland's jurisdiction) as subject to the code (ss 139E, 139G, 139K). The Act specifies that "age-inappropriate content" means " online content that is likely to be unsuitable for children (either generally or below a particular age), having regard to their capabilities, their development, and their rights and interests, including in particular content consisting of: (a) pornography, or (b) realistic representations of, or of the effects of, gross or gratuitous violence or acts of cruelty" (at s139D). The Act provides that appropriate measures for *inter* alia preventing children's access to harmful and age-inappropriate content to be specified in the Online Safety Code (at s139K). The Online Safety Code came into effect in October 2024. The Code is divided into **Part A**, which addresses AVMSD requirements, and **Part B**, which addresses the broader online safety regulation regime. (Coimisiún na Meán, 2025[124]). The Code defines a **child** as a person under the age of 18 years. **Part A Requirements:** Video-sharing platform service providers are required to establish and operate age verification systems for users of video-sharing platforms with respect to content which may impair the physical, mental or moral development of minors". The content is as defined in the AVMSD (at	The Code defines an "age assurance measure" as "a process used to restrict access to a service or to particular features or content of a service that involves estimating or verifying a user's age" (at 11). It further specifies that for the purpose of complying with Part A requirements the term "age verification includes "effective age assurance measures including age estimation" (at 10.6(f)). For the purpose of complying with Part A and Part B requirements, it is specified that "an age assurance measure based solely on self-declaration of age by users of the service shall not be an effective measure" (at 10.6(f), 12.11) The Code further specifies that and personal data of children collected or otherwise generated by video service platform providers in implementing age assurance measures is not to be processed for commercial purposes (at 17.2).	Coimisiún na Meán (**AVMSD & DSA**)

© OECD 2025

Country / Region	Law	Age limit	Purpose / Scope of law	Online age assurance requirement	Administrator
			10.6(f)). **Part B Requirements:** Video-sharing platform service providers whose terms and conditions do not preclude the uploading or sharing of adult-only video content is required to implement effective age assurance to ensure that adult-only video content cannot normally be seen by children (at 12.11). "Adult-only video content" means that consisting of, pornography or "realistic representations of, or of the effects of, gross or gratuitous violence or acts of cruelty" (at 11).		
Italy*	Decreto Legislativo 8 novembre 2021, n. 208 (Legislative Decree no. 208) (Government of Italy, 2021[125])	**18**	*Act transposes the AVMSD.* Video sharing platforms are required to "adopt measures adequate to protect (…) minors from programs, user-generated videos and audiovisual commercial communications that may harm their physical, mental or moral development" (at art. 42.1). Such content is otherwise defined in the Act as including, "**gratuitous or persistent violence or brutal** or pornographic scenes" (at art. 37.1) (emphasis added). The most harmful content is to be subject to the most stringent measures. Measures include establishing "systems to verify, in compliance with the legislation on the protection of personal data, the age of the users of video sharing platforms with regards to content that may harm the physical, mental or morality of minors" (at art. 42.7(f)). The Act does not define **minor**, however Italy's Civil defines the age of majority as 18 (at Book One, art. 2) (Government of Italy, 1942[126]) **Video sharing platform** is as defined in the AVMSD, however the law specifies that it applies to those	The law does not prescribe any particular age assurance methods. A public consultation was launched in March 2024 by AGCOM specifically on age assurance for pornographic websites, however as of March 2025 its status is unclear (see Table A C.1)	Autorità per le garanzie nelle comunicazioni (AGCOM) (**AVMSD & DSA**)

© OECD 2025

Country / Region	Law	Age limit	Purpose / Scope of law	Online age assurance requirement	Administrator
			established in Italy (at art. 41)		
Japan	Japan does not have a law that sets an age assurance requirement. Japan does however have a law specific to protecting children online that sets rules relevant to device level filtering (Government of Japan, 2008[127]).				
Korea	Youth Protection Act (Government of Korea, 1997[128]) Enforcement Decree of the Youth Protection Act (Government of Korea, 1997[129]) Act on Promotion of Information and Communications Network Utilization and Information Protection (the Network Act) (Government of Korea, 2001[130])	**14/16/19**	Korea's online safety framework provides protections for children that either expressly or impliedly require age assurance across a number of factors. <u>Media Harmful to Youth:</u> The Youth Protection Act provides that "any person who intends to sell, rent, distribute, or provide for viewing, watching, or use media materials that are harmful to youth must verify the age and identity" of the receiving party and "not sell, rent, distribute, or provide for viewing, watching, or use to youth" (at art 16). **Youth** is defined as anyone under the age of 19 (at art. 1). "**Material harmful to youth**" is defined the Decree, and includes sexual content (at art. 4 of the Decree) <u>Internet Games</u> The Youth Protection Act, requires providers of Internet Games to request the consent of the parent if the person seeking to register as a member is a minor under the age of 16 (at art. 24) <u>Content Moderation</u> The Network Act provides that when and information communication service provider, provides "a system that processes information in a manner that allows conversation with people using text or voice to a child under the age of 14, the provider must endeavor to ensure that information with inappropriate content is not provided to the child" (art	The Decree establishes methods for determining age (at art. 17). These are: • verifying ID in person or by copying the ID received by fax or mail; • a verifiable electronic signature (provided pursuant to the Electronic Signature Act); • authentication via credit card; • authentication via mobile phone, with additional age verification via a text message transmission or voice auto-response	Ministry of Gender Equality and Family (Youth Protection Laws) Korean Communication Commission(Network Act))

© OECD 2025

Country / Region	Law	Age limit	Purpose / Scope of law	Online age assurance requirement	Administrator
			44-8). The Network Act further prohibits the sale of information that is otherwise determined to be "harmful to youth" for profit, "without fulfilling legal obligations such as age verification (at art. 44-7(5))		
Latvia*	Latvia's law transposing the AVMSD, when dealing with the activities of video sharing platforms and preventing children from accessing material that may impair their "physical, mental or moral development", prescribes measures relevant to developing a code of conduct, and does not specify that "appropriate measures" include age assurance (Government of Latvia, 2010[131])				Nacionālā elektronisko plašsaziņas līdzekļu padome (NEPLP) (**AVMSD)** Patērētāju tiesību aizsardzības centrs (PTAC) (**DSA**)
Lithuania*	Lietuvos Respublikos visuomenės informavimo įstatymas (Public Information Law) (Government of Lithuania, 1996[132])	**18**	Video sharing platforms are required to take measures to protect minors from "programs, user-created videos and commercial audiovisual messages that disseminate information that has a negative impact on minors" (at art 40(1)). Such content is defined elsewhere in the law as being information that "has a negative impact on their physical, mental or moral development, especially related to the dissemination of pornographic and/or **violent information** and information that promotes harmful habits" (at art. 17) (emphasis added). The measures include creating and applying "age verification systems for users of video sharing platforms for information (content) that has a negative impact on minors" (at art 40(2)). The Act does not define **minor**, however Lithuania's Civil Code defines the age of majority as 18 (at art. 2(5)) (Government of Lithuania, 2000[133]). **Video sharing platform** is as defined in the AVMSD, however the law specifies that it applies to those	The law does not prescribe any particular age assurance method. It does note that such a measure must be "adapted and proportionate, taking into account the scope of the service of the video-sharing platform and the nature of the service provided" (at art.40(3)).	Lietuvos Radijo ir Televizijos Komisija (LRTK) (**AVMSD**) Lietuvos Respublikos Ryšių reguliavimo tarnyba (RRT) (**DSA)**

© OECD 2025

Country / Region	Law	Age limit	Purpose / Scope of law	Online age assurance requirement	Administrator
			established in Lithuania (at art. 40)		
Luxembourg*	Loi du 27 juillet 1991 sur les médias électroniques (Law on Electronic Media) (Government of Luxembourg, 1991[134])		*Act transposes the AVMSD.* The law provides that video sharing platforms are to "take appropriate measures to protect minors from programs, user-created videos and audiovisual commercial communications that may harm their physical, mental or moral development" (at art. 28septies (1)(a)). The law does not define what would amount to such harmful content, but does provide that "the most harmful content is subject to the strictest access control measures" and that such measures include implementing and using "systems to verify the age of users" (at art. 28septies (3)(g)) **Minor** is not defined in the law, but Luxembourg's Civil Code defines minor as persons under the age of 18 (at art 388) (Government of Luxembourg, 1803[135]) **Video sharing platform** is as defined in the AVMSD, however the law specifies that it applies to those established in Luxembourg (at art. 23)	The law does not prescribe any particular age assurance methods. The law does provide that the personal data of minors collected or otherwise generated by video sharing platform providers for the purpose of age assurance, must not processed for commercial purposes.	Autorité Luxembourgeoise indépendante de l'audiovisuel (ALIA) (**AVMSD**) L'Autorité de la concurrence (**DSA**)
Netherlands*	The Netherland's Act transposing the AVMSD, when dealing with the activities of video sharing platforms cross-references art. 28b of the AVMSD without specifying any specific measures that should be taken, including age assurance. The Act directs video sharing platforms to develop a code of conduct that include "as appropriate" the measures set out in the AVMSD (Government of the Netherlands, 2008[136])				Commissariaat voor de Media (**AVMSD**) Autoriteit Consument en Markt (ACM) (**DSA**)
Norway*	Norway's law transposing the AVMSD requires service providers to "take measures to ensure that minors do not normally have access to image programs or associated material with seriously harmful content". However, it does not specify if such "measures" include age assurance (Government of Norway, 2015[137]).				Medietilsynet
Poland*	Poland's law transposing the AVMSD, when dealing with the activities of video sharing platforms and preventing children from accessing material that may threaten their "physical, mental or moral development", prescribes that "technical safeguards" should be applied. The law defines these safeguards to include "parental control systems or other appropriate measures" but does not expressly refer to age assurance (at arts. 47o, 47p) (Government of Poland, 1992[138])				Krajowa Rady Radiofonii i Telewizji (KRRiT) (**AVMSD**)

© OECD 2025

Country / Region	Law	Age limit	Purpose / Scope of law	Online age assurance requirement	Administrator
					Prezes Urzędu Komunikacji Elektronicznej (Prezes UKE) (**DSA**)
Portugal*	Poland's law transposing the AVMSD, when dealing with the activities of video sharing platforms and preventing children from accessing material that may impair their "physical, mental or moral development", prescribes a number of "appropriate measures" but does not expressly reference age assurance (see ss69A-69C) (Government of Portugal, 2007[139]).				Entidade Reguladora para a Comunicação (ERC) (**DSA**) Autoridade Nacional de Comunicações (ANACOM) (**AVMSD**)
Slovak Republic*	Zákon o mediálnych službách (Media Services Act) (Government of the Slovak Rebublic, 2022[140])	**18**	*Act transposes the AVMSD.* Video sharing platform providers must take appropriate measures to protect minors from content that may disturb their "physical, psychological or moral development", ensuring that such content is providing in a way that minors cannot see or hear it. Content that contains **gross unjustified violence** (or pornography), can only be provided where technical measures are taken to prevent minor's access (at §48, 62). Appropriate measures for this purpose include the "establishment and operation of a system to verify the age of users" (at §49(1)(i)). The law defines a **minor** as a person younger than 18 years of age (at §62). **Video sharing platform** is as defined in the AVMSD, but the law specifies that it applies to those established in the Slovak Republic (at §7).	The law does not prescribe any particular age assurance method. The does note (at §49(2)) that such a measure must be feasible and appropriate, taking into consideration: • the nature of the content provided; • any damage that the content may cause; • the groups of persons to be protected; • rights and legitimate interests, including those of the video sharing platform provider and the users who uploaded or created the content; and • the general public interest. The law further notes that any measures taken must not "lead to ex ante control measures or to content filtering "that is not otherwise covered in law (at §49(3)), and that the personal data of minors collected or otherwise obtained for assuring age must not be processed for commercial purposes (at §49(4)).	Rada pre vysielanie a retransmisiu (**AVMSD**)
Slovenia*	Zakon o avdiovizualnih medijskih storitvah	**18**	*Act transposes the AVMSD.* Video sharing platform providers must take appropriate	The law does not prescribe any particular age assurance method. The law further notes that any measures taken must not to measures	Agencija za komunikacijska omrežja in storitve

© OECD 2025

Country / Region	Law	Age limit	Purpose / Scope of law	Online age assurance requirement	Administrator
	(ZAvMS) (Act on Audiovisual Media Services) (Government of Slovenia, 2011[141])		measures to protect children from "programs, videos and audiovisual commercial messages that could harm their physical, mental or moral development" (at art. 38b (1)). Content that could harm the physical, mental or moral development of children, is defined as including **gratuitous violence** (as well as pornography) (at art.14(1)). Appropriate measures include "establishment and management of a system for checking the age of users" (at art 38b(7)). The law does not define **child**, but Slovenia's General Child Protection in Audiovisual Media Services Act defines a child as a person who has not reached 18 (Government of Slovenia, 2022[142]).	of "prior control or filtering of content" that is not otherwise covered in law (at art 38b(9)), and that any personal data collected or otherwise obtained for assuring age must only be processed for an age assurance purpose (at art 38b(8)).	Republike Slovenije (AKOS) (**AVMSD & DSA**)
Spain*	General de Comunicación Audiovisual (General Law on Audiovisual Communication) (Government of Spain, 2022[143])	**18**	*Act transposes the AVMSD.* The law requires that providers of video sharing services take measures to protect "minors from programs, user-generated videos and audiovisual commercial communications that may harm their physical, mental or moral development" (at art. 88). Measures are defined to include establishing and operating "age verification systems for users with respect to content that may harm the physical, mental or moral development of minors, which in any case prevent their access to the most harmful audiovisual content, such as **gratuitous violence** or pornography" (at art 89) (emphasis added). Minor is not defined in the law, however Spain's Civil Code (Government of Spain, 1889[144]) defines the age of majority as 18 (at art 315).	The law does not prescribe a particular age assurance method. The law does provide that minor's personal collected or otherwise generated by the video sharing service for the purpose of *inter* alia age assurance may not be processed for commercial purposes (at art. 90).	Comisión Nacional de los Mercados y de la Competencia (**AVMSD & DSA**)
Spain	**Proposal**	In June 2024, the Spanish Council of Ministers approved the Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales (Draft Organic Law for the protection of minors in digital environment). As of March 2025, the law is awaiting parliamentary approval. The law proposes stricter measures for age assurance (including for their enforcement) for content harmful to minors, including pornography, gratuitous violence; and to prohibit certain consumer practices (e.g. random reward systems) (Government of Spain, 2024[145]) (La Moncloa, 2025[146]).			

© OECD 2025

Country / Region	Law	Age limit	Purpose / Scope of law	Online age assurance requirement	Administrator
Sweden*	Radio and Television Act (2010) (Government of Sweden, 2010[147])	**18**	*Act transposes the AVMSD.* The Act requires that "a video-sharing platform provider shall **take appropriate measures** to ensure that user generated videos, television programmes and audiovisual commercial communications that contain detailed depictions of **realistic violence** or pornographic images are not made available in such a manner that presents a significant risk that children will see them, unless this is justified for some special reason" (at Ch 9a, s1) (emphasis added). The law does not prescribe an age assurance method nor specify if "appropriate measures" include age assurance. The law does not explicitly define **child**, however Swedish law considers everyone under 18 to be a child (migrationsverket, 2024[148]).	Unclear, however the law does provide that "personal data collected or otherwise generated by video-sharing platform providers in order to fulfil the requirement for (appropriate) measures (…) may not be processed for commercial purposes".	Mediemyndigheten (**AVMSD**) Post-och telestyrelsen (PTS) (**DSA**)
Switzerland	Loi fédérale sur la protection des mineurs dans les secteurs du film et du jeu vidéo (LPMFJ), entrée en vigueur au 1.1.25 (Federal Act on Audiovisual Media Services) (Government of Switzerland, 2022[149])	**18**	*Act partially transposes the AVMSD.* The law provides that – in the areas of film and video games – providers of on-demand services (Art. 8) and platform services (Art. 20) must take appropriate measures to protect minors from content that may impair their physical, mental, psychological, moral or social development. Such measures must at least include the establishment and operation of an age verification system prior to the initial use of the service (for on-demand services and platform services) and the provision of a parental control system (for on-demand services) or the establishment and operation of a system by which users can report content to the platform service that is unsuitable for minors (for platform services). Content unsuitable for minors is not further defined. While the Act does not define "minor", the Swiss Civil Code defines a minor as a person not yet 18 years of age	The law does not prescribe any particular age assurance method.	Federal Social Insurance Office (JSFVG)

© OECD 2025

Country / Region	Law	Age limit	Purpose / Scope of law	Online age assurance requirement	Administrator
			(Government of Switzerland, 1907[150])		
United Kingdom	Online Safety Act (Government of the United Kingdom, 2023[18])	**18**	The Online Safety Act (OSA) imposes specific duties on service providers regulated by the Act. These duties *inter alia* seek to ensure that children enjoy a higher standard of protection than adults (s1(3)(i)). A **child** is defined as a person under the age of 18 (s236). Regulated service providers are: • **user-to-user** services, (those that host user generated content), and have a link to the United Kingdom (Part 3 service); • **search services** (an Internet service that is, or includes, a search engine), and have a link to the United Kingdom (Part 3 service); and • all **providers of pornographic content**, noting that there is no need for a link to the United Kingdom, but that services which provide pornographic content consisting only of text, or text accompanied by a non-pornographic GIF or emoji are excluded (see s79(1)-(4)) (Part 5 services). (See Table A C.1 for further details on the provisions relevant to pornography) Regulated user-to-user and search services which are likely to be accessed by children in fulfilling their specific safety duties protecting children, must operate the service using proportionate systems and processes designed to prevent children from encountering content that is harmful to them (at s12(3), 29(3)). The Act designates two types of harmful content (see ss60-62): <u>Primary Priority Content (s61)</u> • pornographic content • content which encourages promotes or provides instructions for: ○ suicide	The Act provides that when a service is required to use age verification or age estimation, it must be of such a kind and used in such a way that renders it highly effective at correctly determining whether or not a particular user is a child (s12(6)). The Act specifies that self-declaration alone is not to be regarded as age verification or age estimation (at s230). The Act instructs Ofcom to prepare codes of practice about the various duties under the Act, including the safety duties protecting children (s41(10)(b)). In any code of practice regarding these duties, in deciding whether or not to recommend age assurance, Ofcom must have regard to (at s12(2)): • the principle that age assurance should be effective at correctly identifying the age or age range of users; • the relevant standards set out in the UK's age-appropriate design code ; • the need to strike the right balance between the level of risk / nature and severity of potential harm that age assurance is designed to guard against, and protecting the rights of users and interested persons to freedom of expression within the law. • the principle that more effective kinds of age assurance should be used to deal with higher levels of risk of harm to children; • the principle that age assurance should be easy to use, including by children of different ages and with different needs; • he principle that age assurance should work effectively for all users regardless of their characteristics or whether they are members of a certain group; and • the principle of interoperability between different kinds of age assurance. In April 2025, Ofcom published guidance on "Protecting children from harms online" (Ofcom, 2025[152]), and a statement on industry guidance on effective age checks in January 2025 (Ofcom, 2025[153]). Ofcom does not recommend specific age assurance methods be used, but does recommend, to ensure that their age assurance process are highly effective, services take steps to fulfil the criteria of technical	Ofcom

© OECD 2025

Country / Region	Law	Age limit	Purpose / Scope of law	Online age assurance requirement	Administrator
			○ deliberate self-injury ○ an eating disorders / behaviours associated with an eating disorder <u>Priority Content (S62)</u> • abusive content targeting protected characteristics (race, religion, sex, sexual orientation, disability or gender reassignment) • content inciting hatred against persons of a particular race, religion, sex or sexual orientation; who have a disability; or who have the characteristic of gender reassignment • content that encourages, promotes or provides instructions for an act of serious violence against a person • bullying content • content which depicts real or realistic: ○ serious violence against a person (real or fictional) ○ serious injury of a person (real or fictional) in graphic detail ○ serious violence against an animal (real or fictional) ○ serious injury of an animal (real or fictional) in graphic detail ○ serious violence against a fictional creature or serious injury of a fictional creature in graphic detail; • content that encourages, promotes or provides instructions for a challenge or stunt highly likely to result in serious injury • content that encourages the consumption of a physically harmful substance. **Express age assurance requirement** When **user-to-user** services host "primary priority content"	accuracy, robustness, reliability and fairness. Ofcom's Guidance on highly effective age assurance for part 3 services (Ofcom, 2025[154]) sets out that all providers of Part 3 services are required to carry out children's access assessments to determine whether a service, or part of a service, is likely to be accessed by children. It further notes that under the Act service providers "may only conclude that it is not possible for children to access a service if that service uses a form of age assurance with the result that children are not normally able to access that service or part of it". Accordingly, Ofcom's guidance sets out that "in order to secure the result that children are not normally able to access their service (or a part of it), service providers should deploy highly effective age assurance and implement effective access controls to prevent users from accessing the service (or relevant part of it) unless they have been identified as adults".	

© OECD 2025

Country / Region	Law	Age limit	Purpose / Scope of law	Online age assurance requirement	Administrator
			the child safety duty engages a requirement for age verification or age estimation (or both) to be deployed to prevent children of any age from encountering the content (s12(4)). The age estimation / age verification requirement will not apply in cases where the providers Terms of Service (ToS) indicates that primary priority content (or a particular kind of this content) is prohibited on the service, and that the policy applies to all users of the service (s12(5)). **Implied age assurance requirement** User-to-user services are additionally required to take proportionate measures that can effectively mitigate risk of harm to children on the service, or prevent children from encountering harmful content (other than primary priority content) on their service. Age estimation and age verification are explicitly referenced in the Act as examples of measures which may be taken for the purpose of compliance with these duties (at s12(7)). Additionally, providers of user-to-user and search services must carry out annual children's access assessments (s36(2)) and ad hoc assessments when they make a relevant significant change to the service; where there is evidence that there has been a significant increase in the number of children using the service; or there is evidence that the age verification / age estimation used by the service has reduced in effectiveness (s36(4). All such providers are only entitled to conclude that it is not possible for children to access their service (or particular parts of it) if age estimation / age verification is used on the service with the result that UK children are not able to access the service (or particular parts of it) (s35(2)(5)). *The UK continued to operate a VSP regime, up until March2025 when it was repealed* (Ofcom, 2024[151])		
United States	**Proposed**	**17**	*The Kids Online Safety & Privacy Act has (as of March 2025) passed one chamber of congress (the Senate) and is awaiting a vote in the other (the House).*		

© OECD 2025

Country / Region	Law	Age limit	Purpose / Scope of law	Online age assurance requirement	Administrator
			The bill provides protections aimed at mitigating harm to minors across a variety of online platforms, and an instruction for research into age verification. (United States Congress, 2024[155])		

"*". Denotes EU and EEA Member States that are subject to the provisions of the AVMSD and DSA

© OECD 2025

Annex B. Laws and policies regulating access to social media

Table A B.1 sets out laws and policies that are intended to regulate children's access or use of social media specifically, and that either: i) expressly require age assurance; or ii) contain a measure that implicitly requires age assurance. OECD Member countries that do not have such a law or policy are not included in this table.

Laws that are proposed but so far not enacted are denoted with the label "Proposed" in bold under the Law column (see, e.g., Spain). France's law has passed the legislative process but is still awaiting an administrative step, which is also noted in bold in the Law column, as are initiatives at the policy level that are not enforceable (e.g. Denmark).

The table does not include laws or policies that address online harms across a variety of services, of which one may be social media. These laws and policies are captured in Table A A.1 (on online safety laws), but Table A B.1 points out where such a circumstance exists (e.g. in the United Kingdom). For EU countries, unless the country has a standalone online safety law (e.g. Ireland), this is done with just one reference to the Digital Services Act in the row for the European Union and is not replicated across all EU Member States.

The column "reference age" in this table refers to the maximum age at which the law requires safeguards to be put in place. In some cases, the need for a specific safeguard is mitigated via obtaining parental consent, and so this table also contains a column to reflect those requirements.

Table A B.1. Age-based protections and age assurance requirements relevant to social media

Country / Region	Law	Reference Age	Scope and Purpose of Law	Age Assurance Requirement	Requirement for Verified Parental Consent	Administrator
Australia	Online Safety Amendment (Social Media Minimum Age) Act 2024 (Government of	**16**	The Act amends Australia's Online Safety Act and creates "age restrictions for certain social media platforms" (at s4 of the OSA). These requirements are due to take effect in December 2025 (Australia's eSafety Commissioner, 2025[46]).	The Act does not specifically require age assurance, but the eSafety Commissioner is required to "formulate, in writing, guidelines for the taking of reasonable steps to prevent age-restricted users having accounts	N/a	eSafety Commissioner

© OECD 2025

Country / Region	Law	Reference Age	Scope and Purpose of Law	Age Assurance Requirement	Requirement for Verified Parental Consent	Administrator
	Australia, 2024[156]) Online Safety Act (OSA) (Government of Australia, 2021[90])		An **age-restricted social media platform** is (at s63C OSA) an electronic service that: • has a sole or a significant purpose of enabling online social interaction between 2 or more end-users; • allows end-users to link to, or interact with, some or all of the other end-users; and • allows end-users to post material on the service, The definition does not include services that do not allow their material to be accessible by Australian end users. The Act also provides that the Minister for Communications can make legislative rules specifying that a particular electronic service is or is not an "age-restricted social media platform" (at s63C OSA). An **age-restricted user** is an Australian child who has not yet reached 16 years (at s5 OSA).	with age-restricted social media platforms"; and to promote those guidelines (at 27(1)(qa)(qb) of the OSA). This guidance is (as of March 2025) likely to include age assurance requirements (Australia's eSafety Commissioner, 2025[46]). Failure on behalf of the age-restricted social media platform to take the necessary "reasonable steps" is punishable by a civil penalty. As of March 2025, work to develop such guidance is underway supported by existing research Australia has undertaken on age assurance, as well as the age assurance trial currently ongoing (Australia's eSafety Commissioner, 2025[46]) (Age Assurance Technology Trial, 2025[47]). The Act further provides rules governing the information that can be collected for the purpose of compliance (at ss 63DA, 63DB OSA).		
Australia	Social Media Services Online Safety Code (Class 1A and 1B Material) (2023) (Government of Australia, 2023[157])	**16 / 18**	Australia's Online Safety Act (Government of Australia, 2021[90]) (at s132) provides for the development and registering of enforceable Industry Codes. In June 2023 a specific Industry Code for Social Media Services was registered. This code provides, *inter alia,* that providers of Tier 1 and Tier 2 social media services (see definition below), must: • "terminate an end-users account as soon as reasonable practicable in the event the end-user is (…) known to be using the account in	The code does not set out a specific age assurance requirement but does note that reasonable steps for complying with Measure 6(c) "could include: i) requiring a user to declare their date of birth during the account registration process; ii) implementing age estimation technology to determine a user's age'; or iii) using artificial intelligence tools that help to understand someone's real age". In May 2024, Australia announced that it would run a trial of age assurance	N/a	eSafety Commissioner

© OECD 2025

Country / Region	Law	Reference Age	Scope and Purpose of Law	Age Assurance Requirement	Requirement for Verified Parental Consent	Administrator
			breach of age restrictions concerning the use of the service by an Australian child" (Measure 3(c)(ii)); • "take reasonable steps to prevent an Australian child that is known to be under the minimum age permitted on the service from holding an account on the service, and to remove them from the service" as per the measure above (Measure 6(c)). Providers of Tier 1 and Tier 2 services that permit a young Australian child to be an account holder, "must provide clear and easily accessible information to: a) parents and carers about how to manage the child's access and exposure to Class 1A [CSEA, TVEC] and Class 1B [crime, violence and drug related] material; and b) explain the safety tools and settings on the service in a manner that is easily understood by users of all ages permitted on the service". Providers of Tier 1 social media services that "permit a young Australian child to hold an account on the service must at a minimum: a) have default settings that are designed to prevent a young Australian child from unwanted contact from unknown end-users, including settings which prevent the location of the child being shared with other accounts by default; and b) easy to use tools and functionality that can help safeguard the safety of a young Australian child using the service" (measure 7). <u>Definitions:</u> **Australian child** is an Australian end-user under the age of 18 years. **Social media services** are electronic services that:	technologies (Australia's eSafety Commissioner, 2024[48]). As of March 2025, this trial is ongoing (Age Assurance Technology Trial, 2025[47]).		

© OECD 2025

Country / Region	Law	Reference Age	Scope and Purpose of Law	Age Assurance Requirement	Requirement for Verified Parental Consent	Administrator
			i) have a sole or primary purpose of enabling "online social interaction between 2 or more end-users"; ii) "allows end-users to link to, or interact with, some or all other end-users"; and iii) "allows end-users to post material on the service". (N.b. the Act provides a capacity for legislative rules to further define social media services). A **Tier 1** social media service is one that: provides an Australian end-user with an integrated chat or messaging service that enables end-users to interact via live video streaming; has a primary purpose of general social interaction; has over 30 million total monthly active users globally; has over 3 million Australian total monthly users; enables sharing of materials in all formats; and allows an Australian end-user to create a list of other end-users with which they have a connection in the system, or view and navigate to a list other end-users individual connections, or construct a public or semi-public profile within the system. A **Tier 2** social media service is one that: provides an Australian end-user with an integrated chat or messaging service that does not allow end-users to interact via live video streaming; has a primary purpose of providing a forum for social interaction on a specific topic; has between 5,000,001 and 30 million total monthly active users globally; has between 500,001 and 3 million Australian total monthly users; enables sharing of text, audio, images and video, but not live streaming; and allows an Australian end-user to create a list of other end-users with which they have a connection in the system, or view and navigate to a list other end-users individual connections, or construct a public or semi-public profile within the system.			

© OECD 2025

Country / Region	Law	Reference Age	Scope and Purpose of Law	Age Assurance Requirement	Requirement for Verified Parental Consent	Administrator
			Young Australian child is an Australian end-user under the age of 16 years.			
Colombia	**Proposal**	**14**	Draft Law 176 of 2019 Camera proposes regulations relevant to the use of social networks. It includes a prohibition on children under 14 using social networks, and for express parental consent for publishing or using data for children under 14 years (CELE, 2019[158]). The status of this proposal is unclear.			
Denmark*	**Unenforceable Guidelines** Ethical guidelines for digital service providers (Danish Media Council for Children and Young People, 2025[101])	**18**	These guidelines are ostensibly for all digital services accessed by children but are specifically "aimed at and developed with a focus on (…) social media". The guidelines *inter alia* require that service providers must: • "ensure that illegal content and content that may seriously impair children's development cannot be accessed by children"; • other content be "adapted to the child's age and development, based on an assessment of the content's potential harm and taking into account the child's freedom of expression and information"; • Not use behavioural design to retain child users (e.g. recommender systems, push notifications, visible "likes"); • Activate default time limits, and a "quiet mode" between 10pm and 6am. Further, service providers are required to: • ensure age-appropriateness, through designing, continuously assess, and adapting the service based on the child's age and cognitive and emotional development. • set an age limit that reflects a general consideration for children's protection and use; • ensure that the age limit and target group of the service are clear and justified for children and adults; and • ensure that children who meet the age limit	The guidance requires service providers to "establish and maintain effective, user-friendly, and privacy-protective systems for age verification of users accessing the service". A third party may manage age assurance, provide they comply with the privacy and data protection aspects of the guidance.	N/a	Media Council for Children and Young People

© OECD 2025

Country / Region	Law	Reference Age	Scope and Purpose of Law	Age Assurance Requirement	Requirement for Verified Parental Consent	Administrator
			can access and use the service. Other parts of the guidance relate to protections that would be universally applied, and so would not require age assurance to be effective. Definitions: **Children** are individuals under 18. **Social media** is not defined beyond describing it as offering "visitors the possibility to create and explore profiles and share content".			
European Union	*Digital Services Act (DSA) (2022)* (European Commission, 2022[35])	*The DSA requires "providers of online platforms accessible to minors shall put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service" (at art. 28). This covers but is not specific to social media services, see details in* Table A A.1 (online safety laws).				
France*	**Passed, awaiting EU level approval** LOI n° 2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne (2023) (Sénat, 2023[159])	**15**	Providers of online social network services operating in France are prohibited from allowing children under the age of 15 from opening an account without express parental consent. Where accounts already exist, such consent must be obtained as soon as possible, and parents may request the cancellation of any relevant child account. When a child under the age of 15 opens an account, the service provider is required to give information to both the child and their parents on the risks associated with the use of the service, and any means of prevention. Service providers are also required to provide tools to control the time a child user spends on their service and send regular notifications to child users	Age assurance is to be carried out via technical solutions that are in accordance with a reference framework developed by the French media regulator (ARCOM) in consultation with the French privacy enforcement authority (CNIL). Arcom adopted a framework on technical measures for age assurance specific to online pornography in October 2025 (Arcom, 2024[110]). See further under Annex C.	Parental consent is to be obtained via technical solutions that are in accordance with a reference framework developed by the French media regulator (ARCOM) in consultation with the French privacy enforcement authority (CNIL).	Arcom

© OECD 2025

Country / Region	Law	Reference Age	Scope and Purpose of Law	Age Assurance Requirement	Requirement for Verified Parental Consent	Administrator
			regarding the duration of their session. Definitions: For the purpose of the law **minors** are individuals under the age of 15. An **online social network service** is "any platform that allows end users to connect and communicate with each other, to share content and to discover other users and other content, across multiple devices, especially through chats, posts, videos, and recommendations".			
Ireland*	Online Safety and Media Regulation Act (2022) (Government of Ireland, 2022[160])	Ireland's Act and accompanying Online Safety Code (Coimisiún na Meán, 2025[124]) covers but is not specific to social media services. Accordingly see details of this law in Table A A.1 (online safety laws).				
Spain*	**Proposal**	**16**	In June 2024, the Spanish Council of Ministers approved the Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales (Draft Organic Law for the protection of minors in digital environment). As of March 2025,, the law is awaiting parliamentary approval. The law provides specific social media protections, including introducing a minimum user age of 16 (Government of Spain, 2024[145]) (La Moncloa, 2025[146]).			
United Kingdom	Online Safety Act (Government of the United Kingdom, 2023[18])	The United Kingdom's Online Safety Act regulates the activities of user-to-user services with links to the United Kingdom. User-to-user services are defined as "internet service by means of which content that is generated directly on the service by a user of the service, or uploaded to or shared on the service by a user of the service, may be encountered by another user, or other users, of the service". Ofcom (the administrator of the Act) notes that this includes, but is not limited to, social media (Ofcom, 2024[161]). Accordingly see details of this law in Table A A.1 (online safety laws).				
United States *(Federal)*	**Proposal**	**17**	The Kids Online Safety & Privacy Act has (as of March) passed one chamber of congress (the Senate) and is awaiting a vote in the other (the House). The bill provides specific social media protections for children under 17, and an instruction for research into age verification. (United States Congress, 2024[155])			
United States (*California*)	Protecting Our Kids from Social Media Addiction Act (Senate Bill	**18**	Makes it unlawful for the operator of an "addictive internet-based service" or application to i) provide an addictive feed to a user, or to ii) send notifications between certain evening and schooltime hours	Commencing from 1 January 2027, an operator of an addictive internet-based service must "reasonably determine that the user is not a minor" to provide an	An operator of an addictive internet-based service may obtain verified parental consent to provide an addictive feed, or to send notifications	Attorney-General (Civil penalty)

© OECD 2025

Country / Region	Law	Reference Age	Scope and Purpose of Law	Age Assurance Requirement	Requirement for Verified Parental Consent	Administrator
	976) (California State Legislature, 2024[162])		unless the operator: • does not have actual knowledge that the user is a minor; or • has not reasonably determined that the user is not a minor / or obtained verifiable parental consent to provide an addictive feed / send notifications. Law does not specify a minimum age for holding a social media account with parental consent. <u>Definitions:</u> **Addictive feed** is "an internet website, online service, online application, or mobile application, in which multiple pieces of media generated or shared by users are recommended, selected, or prioritized for display to a user based on information provided by the user, or otherwise associated with the user or the user's device, as specified." It excludes: information or search terms not personally associated with the user or the users device, or previous interactions; information on privacy or technical settings; information the user expressly and unambiguously requested; direct/private messages; or information which is exclusively the next media in a pre-existing sequence. An **addictive internet-based service or application** is "an internet website, online service, online application, or mobile application, including, but not limited to, a "social media platform" (...) that offers users or provides users with an addictive feed as a significant part of the service provided by that internet website, online service, online application, or mobile application" It excludes services whose interactions between users are limited to	addictive feed, or to send notifications during restricted hours. The law does not specify age assurance methods, but provides for the Attorney-General to promulgate relevant regulations. In addition, the law: • requires an operator to annually disclose the number of minor users of its addictive internet based service, and for who the time limited controls are not enabled. • provides that personal information collected for the purpose of assuring age, may not be used for any other purpose or retained, except as necessary under law.	during restricted hours to minors. The law does not specify methods of verified parental consent. When a parent has provided verified consent, the operator must provide a mechanism for the parent to set controls regarding the child's access to the feed, notifications, limit to view likes/feedback, and to set the account to private and set a default feed not based on the child's information. In addition, the law: • requires an operator to annually disclose the number of minor users that it has received verified parental consent for its addictive internet-based service, and to not enable the time limited controls. • expressly notes that verified parental consent should not act to "waive, release, otherwise limit, or serve as a defense to, any claim that the parent, or that the user who is a minor or was a minor at the time of using the internet-based service or application, might have against the operator regarding any harm to the mental health or well-being of the user." • provides that personal information collected for the purpose of verifying parental consent, may not be used for	

© OECD 2025

Country / Region	Law	Reference Age	Scope and Purpose of Law	Age Assurance Requirement	Requirement for Verified Parental Consent	Administrator
			commercial transactions or consumer reviews. **Minor** is an individual under 18 years of age located in California.		any other purpose or retained, except as necessary under law.	
United States *(Colorado)*	Healthier Social Media Use by Youth (House Bill 2401136) (Colorado State Legislature, 2024[163])	**18**	Requires social media to establish a function that either: • provides users under 18 years with information about their engagement with social media, that "helps the user understand the impact of social media on the developing brain, and the mental and physical health of youth users; or • display a (regularly repeating) notification to users who attest to being under 18 years, once that user has spent either a cumulative period of one hour on the platform over a 24 hour period, or is on platform between the hours of 10am and 6pm. The law also establishes a regime for undertaking research on social media and its effect on children. <u>Definitions:</u> The law does not provide an explicit definition of **Minor** but does refer to users under 18 years. **Social media platform** is a "internet-based service, website, or application" that: has more than 100,000 active users in Colorado; allows a person to become a registered user, establish an account, or create a public or semipublic profile for the purpose of allowing users to create, share and view user generated content; enables one or more users to create or post content that can be viewed by other users; and includes a substantial function to allow social interaction between users on the service.	The law does not set out any age assurance requirement, and only refers to users "attesting to being under the age of eighteen".	N/a	Enforcement provisions are not clear on the face of the law. The Office for Information Technology, the Center for Health and Environmental Data, the Department of Public Health and Environment and a temporary stakeholder group are responsible for establishing standards for the notifications.

© OECD 2025

Country / Region	Law	Reference Age	Scope and Purpose of Law	Age Assurance Requirement	Requirement for Verified Parental Consent	Administrator
United States *(Florida)*	An act relating to online protections for minors (House Bill 3) (Florida State Legislature, 2024[164])	**14**	Requires social media platforms to prohibit minors under 14 years of age from creating new or maintaining existing accounts. Users 14 or 15 years of age must have parental consent to open an account. Definitions: **Social media platform** is an "online forum, website or application" that: i) allows users to upload content or view the content/activity of other users; ii) has 10% or more daily active users under 16, and spending on average 2 hours + on the platform; iii) employs algorithms that analyses user data/information to select content; iv) has addictive features (i.e. infinite scrolling, push notifications, personal interactive metrics, auto-play, live streaming).	The law does not specify an age assurance requirement	The law does not specify how parental consent may be verified.	Department of Legal Affairs (actions to be brought under the Florida Deceptive and Unfair Trade Practices Act) Law also establishes a private right of action
United States *(Georgia)*	Protecting Georgia's Children on Social Media Act of 2024 (Senate Bill 351) (Georgia State Legislature, 2024[165])	**16**	Requires social media platforms to verify the age of account holders, and to obtain parental consent to provide account services to minors. Notwithstanding parental consent, social media companies cannot allow minors to open an account if it would be otherwise contrary to law. Law further provides that if the social media company fails to verify age, the special protections relevant to minors must be applied to all users. These are prohibitions on: targeted advertising; collecting data other than for "reasonably necessary" purposes. Definitions: **Minor** is "an individual who resides in (Georgia) and is actually known or reasonable believed by a social media platform to be under the age of 16 years".	Providers of social media platforms are required to make "commercially reasonable efforts to verify the age of account holders with a level of certainty appropriate to the risks that arise from the (platforms) information management practices".	Providers of social media platforms must obtain express parental consent before an account to a minor. The law does not provide exhaustive means of obtaining such consent, but does provide methods include having the parent or guardian: • sign and return a form; • call on a toll-free number provided by the company; • express consent over a video call; • provide government issued ID; • express consent by responding to an email, and "taking additional steps to verify the (parent's) ID". Additionally, verified parental consent	Attorney General (Civil penalty)

© OECD 2025

Country / Region	Law	Reference Age	Scope and Purpose of Law	Age Assurance Requirement	Requirement for Verified Parental Consent	Administrator
			Social media platform is "an online forum that allows an account holder to create a profile, upload posts, view and listen to posts, form mutual connections, and interact publicly and privately with other account holders and users".		can be provided by "any other commercially reasonable method of obtaining consent using available technology".	
United States *(Louisiana)*	Secure Online Child Interaction and Age Limitation Act (Act No. 456) (Louisiana State Legislature, 2024[166])	**16**	Law aims to prevent social media companies from allowing Louisiana minors to open an account on their service without parental consent. Notwithstanding parental consent, social media companies cannot allow minors to open an account if it would be otherwise contrary to law. Law does not specify a minimum age for holding a social media account with parental consent. Law further provides that if the social media company fails to verify the age of Louisiana users, then it must provide the protections relevant to minors to all users. These include prohibitions on: targeted advertising; data collection; and allowing unconnected adults from direct messaging a Louisiana minor. <u>Definitions:</u> **Minors** are individuals that a social media company "reasonably believes or has actual knowledge that the individual is under the age of 16 and is not emancipated or married". **Social media companies** are a person or entity that provides a "social media platform" that is an interactive computer service and has at least 5 million account holders worldwide. **Social media platform:** is a "public or semi-public	Social media companies are required to make "commercially reasonable efforts to verify the age of Louisiana account holders with a level of certainty appropriate to the risks that arise from the information management practices of the social media company". The law does not specify methods for assuring age, but does provide for the Division of Public Protection to set rules on: i) "acceptable processes or means by which a social media company may meet" the age assurance requirements; and ii) "acceptable forms or methods of identification for individuals to verify they are over the age of 16", which may not be limited to a valid government issued ID.	Accounts for Louisiana users under 16 years of age require express parental consent. The law does not provide exhaustive means of obtaining such consent, but does provide methods include having the parent or guardian: • sign and return a form; • call on a toll-free number provided by the company; • express consent over a video call; • provide government issued ID; • express consent by responding to an email, and "taking additional steps to verify the (parent's) ID". Additionally, verified parental consent can be provided by "any other commercially reasonable method of obtaining consent in light of available technology"	Louisiana Division of Public Protection of the Department of Justice (Civil penalty)

© OECD 2025

Country / Region	Law	Reference Age	Scope and Purpose of Law	Age Assurance Requirement	Requirement for Verified Parental Consent	Administrator
			internet-based service or application that has users in Louisiana" and that: i) allows users to interact socially with each other within the service or application; ii) allows users to: construct a public or semipublic profile for the purpose of signing into the service; populate a list of other users; and create and post content viewable by others.			
United States *(New York)*	Stop Addictive Feeds Exploitation (SAFE) for Kids Act (S7694A) (New York State Legislature, 2024[167])	**18**	Law aims to address "dramatic negative effect" of "addictive feeds" on "children and teenagers". It "prohibits social media companies from providing children under 18 with addictive feeds absent parental consent." It does not apply to children's viewing of "non-addictive feeds". It further prohibits covered operators (see definition below) of addictive social media feeds sending New York children overnight notifications between 12am and 6am without verified parental consent. The Act "only imposes obligations on social media companies where the addictive feed is a significant part of their platform, and not on online services that provide such feeds as ancillary features or add-ons, or where users are on the feed for a relatively small portion of their time using the service." <u>Definitions:</u> **Addictive feed** means "a website, online service, online application, or mobile application, or a portion thereof, in which multiple pieces of media generated or shared by users of a website, online service, online application, or mobile application, either concurrently or sequentially, are recommended, selected, or prioritized for display to a user based, in whole or in part, on information associated with the	Absent verified parental consent, it is "unlawful for a covered operator to provide an addictive feed to a covered user" unless "the covered operator has used commercially reasonable and technically feasible methods to determine that if a covered user is not a covered minor". The law provides for the Attorney General to promulgate regulations for identifying commercially reasonable and technically feasible methods for determining "if a covered user is a covered minor". In promulgating regulations, the Attorney General is to have consideration to "the size, financial resources, and technical capabilities of the addictive social media platform, the costs and effectiveness of available age determination techniques for users of the addictive social media platform, the audience of the addictive social media platform, prevalent practices of the industry of the covered operator, and the impact of the age determination techniques on the covered users' safety, utility, and experience".	A covered operator will not be required to assure age to provide an addictive feed to a covered user if "the covered operator has obtained verified parental consent to provide an addictive feed to a covered minor". The law does not prescribe methods for obtaining verified parental consent, but provides for the Attorney General to promulgate regulations in this regard. The law further provides that any information collected for the purpose of verifying parental consent, cannot be used for any other purpose and (unless contrary to law) must be immediately deleted after its use for verifying consent.	Attorney General (Civil Remedies). The Act provides that the Attorney General must establish a website to receive complaints, information and referrals.

© OECD 2025

Country / Region	Law	Reference Age	Scope and Purpose of Law	Age Assurance Requirement	Requirement for Verified Parental Consent	Administrator
			user or the user's device" It excludes: recommendations, prioritization or selections not persistently associated with the user, users device, users previous interactions, or user's privacy or accessibility settings; media the user expressly and unambiguously requested; direct/private messages; media which is exclusively the next media in a pre-existing sequence. **Addictive social media platform** is "a website, online service, online application, or mobile application, that offers or provides users an addictive feed as a significant part of the services provided by such website, online service, online application, or mobile application" A **covered minor** is "a user of a website, online service, online application, or mobile application in New York when the operator has actual knowledge the user is a minor". A **covered operator** is "any person, business, or other legal entity, who operates or provides an addictive social media platform". A **covered user** is "a user of a website, online service, online application, or mobile application in New York, not acting as an operator, or agent or affiliate of the operator, of such website, online service, online application, or mobile application, or any portion thereof". **Minor** is any "individual under the age of 18"	Such regulations should also set out: appropriate levels of accuracy; multiple methods, including at least one that does not rely solely on government ID or allows for anonymity. The law further provides that any information collected for the purpose of determining a covered users age, cannot be used for any other purpose and (unless contrary to law) must be immediately deleted after its use for determining age.		
United States *(Tennessee)*	Protecting Children from Social Media Act (House Bill	**18**	Law creates an obligation for social media companies to verify the age of individuals opening an account, and if the individual is a minor, obtain express parental consent for the minor to become or	The law does not set out how age is to be assured. It does set out that once age "has been verified (…) it is not required to reverify the individual's age".	The law does not set out how parental consent is to be obtained. It does set out that once parental consent "has been verified (…) it is not required to	Attorney General

© OECD 2025

Country / Region	Law	Reference Age	Scope and Purpose of Law	Age Assurance Requirement	Requirement for Verified Parental Consent	Administrator
	1891) (Tennessee State Legislature, 2024[168])		continue as an account holder. For any existing account holders, the social media company must assure age (and if applicable obtain parental consent) within 14 days of any attempt to access an account. If age is not assured the account must be deleted. Law further provides that a social media company must provide parents with means to supervise the minor's account. These means must include "options for the parent to view privacy settings on the account, set daily time restrictions, and implement breaks during which the minor cannot access the account". Definitions: **Minor** is an individual under 18 years of age and not emancipated. **Social media company** is "a person that is an interactive computer service and that provides a social media platform". **Social media platform** is a "website or internet application that: (i) allows a person to create an account; and (ii) enables an account holder to communicate with other account holders and users through posts".	The law does provide that neither the social media company or a third party can retain personally identifying information used to verify age.	reverify the (…) parental consent". Parents must be allowed to revoke consent. The law does provide that neither the social media company nor a third party can retain personally identifying information used to obtain parental consent.	
United States (*Texas)*	Securing Children Online through Parental Empowerment (SCOPE) Act (House Bill 18) (Texas State Legislature,	**18**	Law requires that applicable digital service providers (see definition below) cannot enter into an agreement with a person to create an account, without first registering the person's age. The digital service provider must not allow known minors (see definition below) to alter their age "unless the alternation process involves a commercially reasonable review process".	The law does not prescribe a method for age assurance, beyond requiring the digital service provider to register the person's age.	The law does not prescribe detailed methods for obtaining parental consent. It states that the digital service provider shall verify "using a commercially reasonable method" the identity and relationship to the known minor, for "each person seeking to perform an action on a digital service	Establishes a private right of action (declaratory or injunctive relief) to be brought exclusively by a parent or

© OECD 2025

Country / Region	Law	Reference Age	Scope and Purpose of Law	Age Assurance Requirement	Requirement for Verified Parental Consent	Administrator
	2023[169])		For known minor's, applicable digital service providers must: provide specific privacy and advertising protections; and create and provide parental supervision tools relevant to privacy, commercial transactions, use monitoring and time limits. Two sections in the law setting out protections regarding harmful content and algorithms are currently under temporary court injunction (ss 509.053, 509.056) (as of March 2025) (United States Supreme Court, 2025[170]). Definitions: **Applicable digital service providers** are those who provide "a digital service that: (1) connects users in a manner that allows users to socially interact with other users on the digital service; (2) allows a user to create a public or semi-public profile for purposes of signing into and using the digital service; and (3) allows a user to create or post content that can be viewed by other users of the digital service, including sharing content on: a message board; a chat room; or a landing page, video channel, or main feed that presents to a user content created and posted by other users". **Digital service** is "a website, an application, a program, or software that collects or processes personal identifying information with Internet connectivity". **Digital service provider** is "a person who: (a) owns or operates a digital service; (b) determines the purpose of collecting and processing the personal identifying information of users		as a minor's parent or guardian".	guardian.

© OECD 2025

Country / Region	Law	Reference Age	Scope and Purpose of Law	Age Assurance Requirement	Requirement for Verified Parental Consent	Administrator
			of the digital service". **Known minors** are minors who have (1) registered their age with the digital service provider; or have (2) had their parent / guardian: (i) notify the digital service provider of the minor's age; (ii) successfully dispute the minor's registered age; or (iii) perform a parent / guardian function (under the Act). If either case is true, the digital service provider is to considered to have actual knowledge that minor is less than 18 and must treat the child as a "known minor". **Minor** is a child younger than 18 who has not had "the disabilities of minority removed for general purposes".			
United States (*Utah*)	Social Media Amendments (House Bill 464) (Utah State Legislature, 2024[171])	**18**	Law aims to address "harms to minors from the excessive use of algorithmically curated social media services". It establishes a private right of action for a Utah minor account holder, or their parent/guardian, against a social media company for an adverse mental health outcome that arises "in whole or in part, from the minor's excessive use of the social media company's algorithmically curated social media service". It is a defense if the social media can demonstrate that it: • limits the Utah minor's "use of the algorithmically curated social media service to no more than three hours in a 24 hour period across all devices"; • restricts the Utah minor account holder from accessing the algorithmically curated social media service between 10:30pm and 6:30am;	The law does not set out any age assurance requirements. A companion law addressing *inter alia* age assurance is currently under court injunction (as of March 2025). (Utah State Legislature, 2024[172]) (United States District Court, 2024[173])	The law does not set out methods of parental consent. A companion law addressing *inter alia* parental consent is currently under court injunction (as of March 2025). (Utah State Legislature, 2024[172]) (United States District Court, 2024[173])	Establishes a private right of action

© OECD 2025

Country / Region	Law	Reference Age	Scope and Purpose of Law	Age Assurance Requirement	Requirement for Verified Parental Consent	Administrator
			• requires the Utah minor's parent or legal guardian to consent to the minor's use of the algorithmically curated social media service; • disable engagement driven design elements for a Utah minor's account. <u>Definitions:</u> **Adverse mental health outcome** means "a condition affecting a minor's mental health that is: (i) diagnosable by a licensed mental health care provider; and (ii) acknowledged by professional mental health experts as having a negative impact on a minor's well-being". It expressly includes "depression, anxiety, suicidal thoughts or behaviors, and self-harm thoughts or behaviors". **Algorithmically curated social media service** is a service that "drives user engagement primarily through the use of: (a) a curation algorithm; and (b) engagement driven design elements". **Minor** is "an individual under 18 years old" who has not been emancipated or married. **Social media company** is "an entity that owns or operates a social media service" **Social media service** is a " public website or application that: (i) displays content that is primarily generated by account holders and not by the social media company; (ii) permits an individual to register as an account holder and create a profile that is made visible to the general public or a set of other users defined by the account holder; (iii) connects account holders to allow users to interact socially			

© OECD 2025

Country / Region	Law	Reference Age	Scope and Purpose of Law	Age Assurance Requirement	Requirement for Verified Parental Consent	Administrator
			with each other within the website or application; (iv) makes available to each account holder a list or lists of other account holders with whom the account holder shares a connection within the system; and (v) allows account holders to post content viewable by other users."			

Note: (1) The US state level laws listed in this table routinely provide exceptions when setting out the definition of a "social media platform" to exclude services with a predominant function such as email, video conferencing, or commercial transactions. For brevity, these exceptions are not reflected in this table. (2) "*": Denotes EU and EEA Member States that are subject to the provisions of the DSA

© OECD 2025

Annex C. Laws regulating access to pornography

Table A C.1 sets out laws relevant to preventing children's access to pornography. They include: i) criminal laws; ii) broadcasting/media laws; and iii) laws specific to pornography on the Internet. As this research primarily seeks to capture laws that regulate the online provision of pornography, where a country has such a law in place, only that law that is described in the table below, even if a relevant provision exists in a broader broadcasting or criminal law. The only exception is where the law regulating online access works in tandem with a criminal or broadcasting law (e.g. Australia).

For OECD Member countries that do not have a law regulating children's access to pornography online, the provisions in the relevant law(s) (usually broadcasting or criminal law) are set out.

Table A C.1. Age-based protections and age assurance requirements relevant to accessing pornography

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
Australia	National Classification Code (Government of Australia, 2013[174]) Online Safety Act (Government of Australia, 2021[90])	18	The National Classification Code establishes a range of classifications for sexually explicit material that is not suitable for children. These classifications include: X18+, Restricted Content, Category 1 Restricted, and Category 2 Restricted. Each category describes sexual acts of varying levels. For instance: "real depictions of actual sexual activity between consenting adults in which there is no violence" (x18+); to "sexual or sexually related activity between consenting adults in a way that is likely to cause offence to a reasonable adult" (Restricted Category 2). Australia's Online Safety Act deems material that falls into the above categories as "class 2 material" (at s107), and specifies that procedures for dealing with such material can be specified in codes (at s 138). As of March 2025, codes to deal with class 2 material, are under development, and are at consultation stage	There is no current online age assurance requirement. The eSafety Commissioner is (as of March 2025) running an age assurance trial to test the efficacy of age verification and age estimation technologies in protecting children from encountering *inter alia* online pornography (Australia's eSafety Commissioner, 2024[48]). At the same time, the Commissioner is developing industry codes that will regulate class 2 material (Australia's eSafety Commissioner, 2024[38]) (Online Safety Australia, 2025[39]). Guidance from the eSafety Commissioner notes that while the trial will not specifically inform the creation of the Codes, consideration will be given to how outputs from the trial can inform and support the development of the Codes. Adding context not only to "what industry is expected to do (e.g., take reasonable and appropriate steps to confirm users' age) and when or where they should do it" but also	Australian Communications and Media Authority (ACMA) eSafety Commissioner

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
			(Australia's eSafety Commissioner, 2024[38]) (Online Safety Australia, 2025[39]) At present these draft codes envisage age assurance requirements for pornography (Online Safety Australia, 2025[39]). .	guidance on "the how (e.g., by informing what reasonable and appropriate steps for compliance may be best within the Australian context)" (Australia's eSafety Commissioner, 2024[38]). The current consultation drafts of the phase 2 codes refer to age assurance measures needing to be "technically feasible and reasonably practicable" (Online Safety Australia, 2025[39]).	
Austria*	Audiovisuelle Mediendienste-Gesetz (AMD-G) (Federal Act on Audiovisual Media Services) (Government of Austria, 2020[93])	**18**	*Act transposes the AVMSD.* The law provides that content in audiovisual media services that may impair the physical, mental or moral development of minors may only be provided by the media service provider in such a way that it cannot normally be perceived by minors (at s39). The law further notes that the most harmful content, in particular that which depicts sexual acts, may only be made available if "measures such as age verification systems or comparable access control measures ensure that minors cannot normally view such content" (at s. 39); and that content predominantly limited to sexual acts (as defined in s39), must be subjective to effective access control by means of age verification (at s 54e). **Minor** is not defined in the Act however the Austrian Civil Code defines a minor as a person not yet 18 years of age (at s21) (Government of Austria, 2018[94]). **Video sharing platform** is as defined by the AVMSD.	The law does not prescribe any particular age assurance method.	KommAustria
Belgium*	Loi relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale (Law relative to audiovisual media services in the bi-lingual region of Brussels Capital) (Government of	**18**	*Act transposes the AVMSD.* The law provides that video-sharing platform service providers are to take appropriate measures to protect minors from "programmes, user-generated videos and audiovisual commercial communications that may be harmful to their physical, mental or moral development" and ensuring that such content is only made available under conditions that prevent minors from seeing or hearing it. Pornography and gratuitous violence are considered the most harmful content (at art. 29/1).	The law does not prescribe any particular age assurance method. The law does provide that any personal data from children collected or generated for the purpose of age verification cannot be processed for commercial purposes (at art. 29/1, § 2 (3)).	Institute for Postal Services and Telecommunications (BIPT)

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
	Belgium, 2017[95])		Appropriate measures include "setting up and using systems for verifying the age of users" (at art. 29/1, § 2 (3)) **Minor** is not defined in the law however the Belgium Civil Code defines a minor as a person not yet 18 years of age (at s488) (Government of Belgium, 1804[96]). **Video sharing platform** is as defined by the AVMSD.		
Canada	Ratings Classifications (Canadian Broadcast Standards Council, 2024[175])	**18**	Canada does not have a law expressly dealing with access to pornography, either in general or online. Prohibitions on children viewing pornography is captured under the broadcasting classification scheme, which rates content that includes "explicit portrayals of sex/nudity" as for audiences 18 and over only.	N/a	Radio-television and Telecommunications Commission / Broadcast Standards Council
Chile	Normas Generales sobre Contenidos de las Emisiones de Televisión (General Rules on Content of Television Broadcasts) (Government of Chile, 2016[176])	**18**	Chile does not have a law regulating pornographic content online. The law regulating pornographic content on television, defines pornographic content as "abusive or crude exposure of sexuality or the display of obscene images, expressed in terms of genitals, lasciviousness and absence of context" (at art. 1(c)), and prohibits the showing of such content to persons under the age of 18 (at art. 5).	N/a	Consejo Nacional de Televisión
Colombia	Resolución 5050 de 2016 CRC (Comisión de Regulación de Comunicaciones, 2016[177])	**18**	Colombia does not have a law regulating pornographic content online. The law regulating television broadcasting prohibits the screening of pornography entirely on public television (at art. 16.4.5.2), and, under the heading "special programming for adults" limits pornography on subscription television to paid per view / video on demand services, or so that it is "only viewed at the discretion of the subscriber". While the law does not define child, Colombia's Code on childhood and adolescence defines a child as a person aged	N/a	Comisión de Regulación de Comunicaciones (CRC)

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
			between 0-12 years, and an adolescent as any person between 12 and 18 (at art 3) (Government of Colombia, 2006[178]).		
Costa Rica	Protección de la niñez y la adolescencia frente al contenido nocivo de internet y otros medios electrónicos (Law on the Protection of Children and Adolescents from Harmful Content on the Internet) (Law No. 8934) (2011) (Government of Costa Rica, 2011[179])	**18**	The law limits access to content considered harmful to minors "moral or psychological integrity" over the Internet, and explicitly covers pornography. The law is aimed at providers of physical infrastructure and requires those providers to install filters or blocks on such content, or display warnings. Definitions: Material **intended for minors** is that "which can be used by minors, regardless of whether it is exclusive or not, or the type of activity to which the premises or establishment are dedicated". **Minor** is not defined in this law however Costa Rica's Civil Code defines them as individuals who have not yet reached 18 (at art 37) (Government of Costa Rica, 1985[180]). **Pornography** is "material of a visual representation or illustration of a person, in real or simulated form, in an exhibition, activity or act sexual".	N/a	Superintendencia de Telecomunicaciones (SUTEL)
Czechia*	Zákon o službách platforem pro sdílení videonahrávek a o změně některých souvisejících zákonů (zákon o službách platforem pro sdílení videonahrávek (Video Sharing Platform Services Act) (Government of	**18**	*Act transposes the AVMSD.* The law provides that video-sharing platform service providers are to adopt measures to protect, "minors from programmes, user-generated videos and commercial communications which might impair their physical, mental, or moral development", and that such content "are only made available in such a way as to ensure that minors will not normally hear or see them". The law further notes that "measures to protect minors include, in particular, age verification tools or other technical measures" (at § 7(1)). The law further provides that "the most objectionable content that may impair the physical, psychological or moral development of	The law does not prescribe any particular age assurance method, but does note that in applying any of the "strictest measures" – which includes age verification – that the measure must be "feasible and proportionate to the scale and nature of the video-sharing platform service provided and shall not lead to filtering of uploaded content or to preliminary control measures" (at § 8(1)). The law further provides that any personal data from children collected for the purpose of establishing *inter alia* age assurance mechanisms, must not "be processed for commercial purposes, in particular, for direct marketing, profiling and behavioural advertising" (at § 9).	Rada pro rozhlasové a televizní vysílání (RRTV)

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
	Czechia, 2022[97])		minors, such as **pornography** or gross self-inflicted violence, shall be subject to the strictest measures to control access" (at § 8(2)), which includes "age verification" (at § 8(3)(f)). **Minor** is not defined in this law however Czechia's Civil Code defines them as individuals who have not yet reached 18 (at § 30) (Government of Czechia, 2012[98]). **Video sharing platform** is as defined in the AVMSD, however the law specifies that it applies to those established in Czechia (at §.3)		
Denmark*	Straffeloven (Criminal Code) (Government of Denmark, 2021[181])	**16**	The law transposing the AVMSD into Danish law does not expressly deal with pornography. See Table A A.1 for details of that law. Denmark's Criminal Code regulates children's access to pornography prohibiting the sale of "obscene images or objects to a person under the age of 16" (at s234).	See Table A A.1, however it is unclear if the provisions of the law transposing the AVMSD apply to pornography.	Department of Justice
Estonia*	Meediateenuste seadus (Media Services Act) (Government of Estonia, 2010[102]) Karistusseadustik (Penal Code) (Government of Estonia, 2001[182])	**16/18**	Estonia's law transposing the AVMSD (the Media Services Act) does not expressly deal with pornography on video sharing platforms. It does provide that "media service providers" (as defined in §4 and including television and radio) cannot transmit programs that "significantly harm the physical, mental or moral development of minors (…) especially programs that contain pornography" (at § 19). Minor is not defined in the Act, however Estonia's child protection law establishes that a child is every person under 18 (at §3(2)) (Government of Estonia, 2014[183]). Estonia's Penal Code (at §179) prohibits "handing over, showing or otherwise knowingly making available a pornographic work or its reproduction to a person younger than sixteen years of age".	N/a	Tarbijakaitse ja Tehnilise Järelevalve Amet (TTJA) Department of Justice
European Union	*Audiovisual Media Services Directive (AVMSD)*	***18***	*Article 28b of the AVMSD provides that "Member States shall ensure that video-sharing platform providers under their jurisdiction take appropriate measures to protect (…) minors*	*Article 28b specifies that the most harmful content shall be subject to the strictest access control measures. As appropriate, those measures inter alia include, "establishing and operating age*	*European Commission*

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
	(European Commission, 2018[34])		*from programmes, user-generated videos and audiovisual commercial communications which may impair their physical, mental or moral development in accordance with Article 6a(1)"* *Article 6a(1) of the AVMSD requires "Member States to take* ***appropriate measures*** *to ensure that audiovisual media services provided by media service providers under their jurisdiction which may impair the physical, mental or moral development of minors are only made available in such a way as to ensure that minors will not normally hear or see them". The most harmful content, such as gratuitous violence (as addressed in* Table A A.1*) and* ***pornography*** *are to be subject to the strictest measures." (emphasis added).* *Definitions:* ***Minor*** *is not defined in the AVMSD, however the European Commissions Better Internet for Kids Policy defines children as individuals under 18 years* (European Commission, 2022[103]). ***Video-sharing platform*** *services are those "where the principal purpose of the service or of a dissociable section thereof or an essential functionality of the service is devoted to providing programmes, user-generated videos, or both, to the general public, for which the video-sharing platform provider does not have editorial responsibility, in order to inform, entertain or educate, by means of electronic communications networks (…)and the organisation of which is determined by the video-sharing platform provider, including by automatic means or algorithms in particular by displaying, tagging and sequencing".*	*verification systems for users of video-sharing platforms with respect to content which may impair the physical, mental or moral development of minors".* *Article 6a specifies that appropriate measures "may include selecting the time of the broadcast,* ***age verification tools*** *or other technical measures" (emphasis added)* *Any measures taken are to be proportionate to the potential harm. Any personal data of minors collected or otherwise generated by media service providers for the purpose of implementing appropriate measures are not to be processed for commercial purposes.*	*Member State supervisory authorities*
Finland*	Kuvaohjelmalaki (Image Program Act) (Government of Finland, 2011[104])	**18**	*Act transposes the AVMSD.* The law provides that video sharing platforms "must take appropriate measures to protect children from such image programs that may be harmful to the child's development" (at s7A).	The law does not expressly define "appropriate measures" to include age assurance. It does note that any measures must be "proportionate to the nature of the video programs in question and the potential harm caused by them, taking into account the size of the video sharing platform service and the nature of the service offered". And that "the	Traficom

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
			Programs harmful to a child's development are those that due to "violence or sexual content, or by causing anxiety" can cause harm to a child's development. In evaluating harmfulness, consideration should be given to the context in which the content is presented (at s15). **Minor** is not defined in the law, however Finland's Act on Guardianship defines a minor as persons under the age of 18 (at s2) (Government of Finland, 1999[105]).	measures must not lead to pre-checking of content or filtering applied to uploading to the platform" (at s7a).	
France*	SREN Loi (Government of France, 2024[107]) Code Pénal (Government of France, 1810[108])	**18**	The law transposing the AVMSD does not expressly deal with pornography (see Table A A.1for details of that law). Frances SREN law, however, deals explicitly with online pornography, requiring that it not be made available to children and establishing requirements for a minimum technical standard for age assurance to be developed (at art. 1). It further creates financial penalties for online pornography providers who do not comply with these standards (at art. 2) France's Penal Code prohibits "manufacturing, transporting, distributing by any means whatsoever and on any medium" a pornographic message or pornographic images. It expressly provides that the offence will be constituted even if the minor's access resulted from a self-declaration indicating that they are at least 18 years old (at art. 227-24).	Arcom adopted a framework on technical measures for age assurance specific to online pornography in October 2025 (Arcom, 2024[110]), and age assurance is now mandatory on pornographic sites under Arcom's jurisdiction. Should a site fail to verify age, Arcom is empowered to impose financial sanctions, block and de-list pornographic sites left accessible to minors in violation of French criminal law. Sites in scope of the jurisdiction are those established in France or outside the European Union, as well as those located in the European Union provided that they appear on a ministerial decree (Arcom, 2025[50]). The prescribed manner for assuring age is set out in a technical reference document, that Arcom developed in conjunction with CNIL (the privacy enforcement authority) (Arcom, 2024[110]). The requirements are: • The age assurance provider must be legally and technically independent from the platform service • The platform service must not access and process the users' data collected for the verification. • The age assurance provider must not store the users' data and collect official ID documents, unless the system is used to generate reusable proof of age • No personal data of the users can be stored by any third party, unless requested to do so by the user. • The age assurance provider must allow users to challenge the result of the analysis, and provide information on redress mechanisms.	Arcom Ministry of Justice

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
Germany*	Jugendschutzgesetz (JuSchG) (Youth Protection Act) (Government of Germany, 2002[112]) Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien (Jugendmedienschutz-Staatsvertrag – JMStV) (Interstate Treaty on the Protection of Minors in the Media) (Government of Germany, 2002[111])	**18**	*Act transposes the AVMSD.* The JuSchG provides that all pornographic content is seriously harmful to minors and therefore must not be accessed by children and young people (§ 15 (2)). The Act requires video sharing providers to take "appropriate measures to protect children and young people from offers (of content) that are detrimental to their development" (at § 5a(1)). Establishing and operating an age verification system amounts to an appropriate measure (at § 5a(2)). The law defines a **child** as someone who is not yet 14, and a young person as someone between the age of 14 and 18 (at §3). The law does not define the particular content that would be detrimental to children's development, but guidance from the BPjM on what is "indexed" for the purpose of requiring age verification includes pornography (Bundesprüfstelle für jugendgefährdende Medien, 2024[113]).	The law does not prescribe any particular age assurance methods. However, KjM (Germany's Commission for Youth Media Protection) has issued guidance on age assurance, recommending that any system comprise both an identification component, and an authentication component (Kommission für Jugendmedienschutz, 2024[41]).	Bundeszentrale für Kinder- und Jugendmedienschutz (BzKJ) Kommission für Jugendmedienschutz (KjM)
Greece*	Law 4779 of 2021 (Government of Greece, 2021[116])	**18**	*Act transposes the AVMSD.* The law states that video sharing platforms "must take appropriate measures to protect minors" from videos and programs that "may have a negative effect on their physical, mental or moral development" (at art 32(1)). The law specifies that for the purpose of protecting minors, "the most harmful content is subject to the strictest access control measures, which include the "installation and operation of systems for verifying the age of users of the platform, in order to prevent access by minors (at s32(6))". The "most harmful content" is defined as including "gratuitous violence and	The law does not prescribe any particular age assurance methods. The law does provide that the ESR can establish guidance / procedures for complying with any of the "appropriate measures" (and so, including age assurance) (at art. 32.8); and that the ESR can ask video sharing platforms for information on *inter alia* age assurance systems (at art. 32.10). The law further provides that any personal data from children collected for the purpose of establishing *inter alia* age assurance mechanisms, must not be "subject to processing for commercial purposes" (at art. 32.7).	National Council for Radio & Television (ESR)

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
			pornography" (at art. 9.1) (emphasis added). **Minor** is not defined in the law, but Greece's Civil Code (at art. 127) defines a minor as persons under the age of 18 (Government of Greece, 1946[117]). **Video sharing platform** is as defined in the AVMSD, but the law specifies that it applies to those established in Greece (at art. 31)		
Hungary*	1997. évi XXXI. törvény a gyermekek védelméről és a gyámügyi igazgatásról (Child Protection Act) (Government of Hungary, 1997[184])	**18**	The law transposing the AVMSD into Hungarian law does not expressly deal with pornography. See Table A A.1 for details of that law. The Child Protection Act prohibits pornography being made available to minors (at §6/A), minors are defined under the Civil Code as persons under the age of 18 (at §2.10) (Government of Hungary, 1997[184]) (Government of Hungary, 2013[119]).	See Table A A.1, however it is unclear if the provisions of the law transposing the AVMSD apply to pornography.	Ministry of Culture & Innovation
Iceland*	Lög um fjölmiðla (Act on the Media) (Government of Iceland, 2011[121])		*Act transposes the AVMSD.* Video sharing platforms are required to "take appropriate measures to protect children from content, user-generated content and commercial messages that may harm their physical, mental or moral development" (at art 36.a). Such content is noted to be in particular "content that includes **pornography** or gratuitous violence" (at art. 28) (emphasis added). Such measures include establishing and operating "an age verification system" (at art 36.d.g) **Minor** is not defined in the law, however Iceland's Law of Jurisdiction, defines the age of majority as 18 (Government of Iceland, 1997[122])	The law does not prescribe any particular age assurance methods. The law does provide that any personal data from children collected for the purpose of establishing *inter alia* age assurance mechanisms, must not be used for commercial (at art. 36).	fjolmidlanefnd
Ireland*	Online Safety and Media Regulation Act (Government of	**18**	Ireland's Act, both transposes the AVMSD and establishes a broader online safety regulatory regime. The Act provides for the CnaM to make an Online Safety Code, and designate online service providers (including video-service providers under	The Code defines an "age assurance measure" as "a process used to restrict access to a service or to particular features or content of a service that involves estimating or verifying a user's age" (at 11).	Coimisiún na Meán (CnaM)

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
	Ireland, 2022[123])		Ireland's jurisdiction) as subject to the code (ss 139E, 139G, 139K). The Act specifies that "age-inappropriate content" means " online content that is likely to be unsuitable for children (either generally or below a particular age), having regard to their capabilities, their development, and their rights and interests, including in particular content consisting of: (a) **pornography**, or (b) realistic representations of, or of the effects of, gross or gratuitous violence or acts of cruelty" (at s139D) (emphasis added). The Act provides that appropriate measures for *inter* alia preventing children's access to harmful and age-inappropriate content to be specified in the Online Safety Code (at s139K). . The Online Safety Code came into effect in October 2024. The Code is divided into **Part A**, which addresses AVMSD requirements, and **Part B**, which addresses the broader online safety regulation regime. (Coimisiún na Meán, 2025[124]). The Code defines a **child** as a person under the age of 18 years. **Part A Requirements:** Video-sharing platform service providers are required to establish and operate age verification systems for users of video-sharing platforms with respect to content which may impair the physical, mental or moral development of minors". The content is as defined in the AVMSD (at 10.6(f)). **Part B Requirements:** A video-sharing platform service provider whose terms and conditions do not preclude the uploading or sharing of adult-only video content is required to implement effective age assurance to ensure that adult-only video content cannot normally be seen by children (at 12.11).	It further specifies that for the purpose of complying with Part A requirements the term "age verification includes "effective age assurance measures including age estimation" (at 10.6(f)). For the purpose of complying with Part A and Part B requirements, it is specified that "an age assurance measure based solely on self-declaration of age by users of the service shall not be an effective measure" (at 10.6(f), 12.11) The Code further specifies that any personal data of children collected or otherwise generated by video service platform providers in implementing age assurance measures is not to be processed for commercial purposes (at 17.2).	

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
			"Adult-only video content" means that consisting of, **pornography** or "realistic representations of, or of the effects of, gross or gratuitous violence or acts of cruelty" (at 11).		
Israel	Penal Code (Government of Israel, 1977[185])	**18**	There is no law dealing with the distribution of pornography online. The Penal Code prohibits the publication, public display, or display in a private place accessible to individuals under 18 of obscene material (at s214).	N/a	Ministry of Justice
Italy*	Decreto Legislativo 8 novembre 2021, n. 208 (Legislative Decree no. 208) (Government of Italy, 2021[125])	**18**	*Act transposes the AVMSD.* Video sharing platforms are required to "adopt measures adequate to protect (…) minors from programs, user-generated videos and audiovisual commercial communications that may harm their physical, mental or moral development" (at art. 42.1). Such content is otherwise defined in the Act as including, "gratuitous or persistent violence or brutal or **pornographic** scenes" (at art. 37.1) (emphasis added). The most harmful content is to be subject to the most stringent measures. Measures include establishing "systems to verify, in compliance with the legislation on the protection of personal data, the age of the users of video sharing platforms with regards to content that may harm the physical, mental or morality of minors" (at art. 42.7(f)). The Act does not define **minor**, however Italy's Civil Code defines the age of majority as 18 (at Book One, art. 2) (Government of Italy, 1942[126]) **Video sharing platform** is as defined in the AVMSD, however the law specifies that it applies to those established in Italy (at art. 41)	The law does not prescribe any particular age assurance methods. In March 2024, AGCOM launched a public consultation (Resolution No. 61/24/CONS) for the approval of a final decision setting out technical age verification measures to be implemented by operators of websites and video-sharing platforms disseminating pornographic content. The consultation closed in April 2024, and as of March 2025 the webpage is no longer active, and the status of the consultation is unclear (European Audiovisual Observatory, 2024[42]).	Autorità per le garanzie nelle comunicazioni (AGCOM)
Japan	Criminal Code (Government of Japan, 1908[186])	**N/a**	Japan's Criminal Code in general prohibits pornography, including its distribution via electronic communications (at art. 175).	N/a	Ministry of Justice
Korea		**N/a**	Korea's Penal Code in general prohibits the distribution, sale, lease, or public exhibition of obscene documents, pictures, films,	See details in Table A A.1.	Ministry of Justice

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
	Penal Code (Government of Korea, 1953[187]) Act on Promotion of Information and Communications Network Utilization and Information Protection (the Network Act) (Government of Korea, 2001[130])		or other objects; as well as manufacturing, possessing importing or exporting obscene materials for these purposes (at art 243, 244) The Network Act likewise prohibits the distribution, sale, rent or public display, via information communications network, obscene symbols, words, sounds, images, or videos (at art. 44-7(1)). Despite these prohibitions, the Korean Law does regulate youth (<19) access to harmful materials including pornography. See details in Table A A.1.		Korean Communication Commission
Latvia*	Bērnu tiesību aizsardzības likums (Law on the Protection of Children's Rights) (Government of Latvia, 1998[188])	**18**	The law transposing the AVMSD into Latvian law does not expressly deal with pornography, nor specify that "appropriate measures" include age assurance. See Table A A.1 for details of that law. Latvia's Law on the Protection of Children's Rights, prohibits, showing, selling, giving or promoting, toys and video recordings, computer games, newspapers, magazines and other types of publications in which *inter alia* pornography is promoted. It is further prohibited to allow children to access pornographic material (at s50). A child is defined as a person under the age of 18 (s3)	N/a	Ministry of Welfare
Lithuania*	Lietuvos Respublikos visuomenės informavimo įstatymas (Public Information Law) (Government of Lithuania, 1996[132])	**18**	Video sharing platforms are required to take measures to protect minors from "programs, user-created videos and commercial audiovisual messages that disseminate information that has a negative impact on minors" (at art 40(1)). Such content is defined elsewhere in the law as being information that "has a negative impact on their physical, mental or moral development, especially related to the dissemination of **pornographic** and/or violent information and information that promotes harmful habits" (at art. 17) (emphasis added). The measures include creating and applying "age verification	The law does not prescribe any particular age assurance method. It does note that such a measure must be "adapted and proportionate, taking into account the scope of the service of the video-sharing platform and the nature of the service provided" (at art.40(3)).	Lietuvos Radijo ir Televizijos Komisija (LRTK)

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
			systems for users of video sharing platforms for information (content) that has a negative impact on minors" (at art 40(2)). The Act does not define **minor**, however Lithuania's Civil Code defines the age of majority as 18 (at art. 2(5)) (Government of Lithuania, 2000[133]). **Video sharing platform** is as defined in the AVMSD, however the law specifies that it applies to those established in Lithuania (at art. 40)		
Luxembourg*	Code pénal (Government of Luxembourg, 1879[189])	**16**	The law transposing the AVMSD into Luxembourg law does not expressly deal with pornography. See Table A A.1for details of that law. Luxembourg's Penal Code prohibits the public display, selling or distributing of "indecent writings, images, figures or objects likely to disturb [the child's] imagination" to children under the age of sixteen (at art. 385bis).	N/a	Ministry of Justice
Mexico	Código Penal Federal (Government of Mexico, 1931[190])	**18**	Mexico does not have a law regulating pornographic content online. The Criminal Code (at s200) prohibits the selling, distributing, exhibition, circulating or offering, to "minors under eighteen years of age, books, writings, recordings, films, photographs, printed advertisements, images or objects of a pornographic nature, real or simulated" through physical or "any means". The Code specifies that "pornographic or harmful material shall not be deemed to be material that is intended or intended for scientific, artistic or technical dissemination, or where appropriate, sexual education, education on reproductive function, prevention of sexually transmitted diseases and teenage pregnancy, provided that it is approved by the competent authority".	N/a	Ministry of Justice
Netherlands*	Mediawet (Media Act) (Government of the	**16**	While the Netherland's Act transposing the AVMSD does not expressly deal with pornography on video sharing platforms (see under Table A A.1), the law does provide protections for minor's	N/a	Commissariaat voor de Media

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
	Netherlands, 2008[136])		audiovisual media services generally. The Act provides that "audiovisual media content that may harm the physical, mental or moral development of persons under the age of sixteen" can only be made available in a manner that prevents persons under 16 from seeing or hearing it. The most harmful content is defined to include pornography (at art. 4.1a)		
New Zealand	Films, Videos, and Publications Classifications Act (Government of New Zealand, 1993[191])	**18**	New Zealand does not have a law expressly dealing with access to pornography online. The broadcasting law does prohibit the supply, distribution, exhibition, or display of objectionable material to persons under the age of 18 (at ss126,127). Material is "objectionable if it describes, depicts, expresses, or otherwise deals with matters such as" *inter alia* sex (at s3).	N/a	Classification Office
Norway*	Lov om beskyttelse av mindreårige mot skadelige bildeprogram mv (Act on the Protection of Minors Against Harmful Image Programs etc) (2015) (Government of Norway, 2015[137])	**18**	*Act transposes the AVMSD.* Service providers are required to "take measures to ensure that minors do not normally have access to image programs or associated material with seriously harmful content". **Harmful content** is defined as depictions that "can be emotionally upsetting or cognitively disruptive to the well-being of minors". **Seriously harmful content** is defined as depictions "that can be highly emotionally upsetting or cognitively disturbing for the well-being of minors, particularly **intimate depictions of sexual activity,** gross violence and other highly disturbing or frightening themes." (emphasis added) Service providers are required to "offer measures that can be activated by guardians or others in the guardian's place, to ensure that minors do not normally gain access to image programs or associated material with harmful content", however the law does not specify if "measures" include age assurance.	. N/a	Medietilsynet

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
			Minors are "persons who have not reached the age of 18".		
Poland*	Ustawa o radiofonii i telewizji (The Broadcasting Act) (Government of Poland, 1992[138])	**18**	*Act transposes the AVMSD.* Video sharing platforms are prohibited from posting broadcasts, user-generated videos or other communications "that threaten the proper physical, mental or moral development of minors, in particular by containing **pornographic content** or unjustifiably exposing violence without applying effective technical safeguards" (at art. 47.o) (emphasis added). The law further defines "technical safeguards" to include "parental control systems or other appropriate measures", but does not expressly refer to age assurance (at art. 47p). The Act does not define **minor**, however Poland's Civil Code defines the age of majority as 18 (at art. 10) (Government of Poland, 1964[192]).	N/a	Krajowa Rady Radiofonii i Telewizji (KRRiT)
Portugal*	Lei da Televisão e dos Serviços Audiovisuais a Pedido (Act on Television and on-demand Audiovisual Services) (Government of Portugal, 2007[139])	**18**	*Act transposes the AVMSD.* Video sharing platforms are required to take appropriate measures to protect minors from "programmes, user-generated videos and audiovisual commercial communications that may harm their integral physical, mental or emotional development" (at art. 69A). The law provides a list of appropriate measures, but age assurance is not included in this list (see art. 69C). Such content is defined elsewhere in the law as being information that is "likely to manifestly, seriously and gravely harm the free development of the personality of children and young people or their image and the privacy of their private and family life, in particular those containing **pornography** or gratuitous violence" (at art. 27) (emphasis added). The Act does not define **minor**, but Portugal's Civil Code defines a minor as any person not yet 18 years of age (at art. 122) (Government of Portugal, 1966[193])	N/a	Autoridade Nacional de Comunicações (ANACOM)

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
Slovak Republic*	zákon o mediálnych službách (Media Services Act) (Government of the Slovak Rebublic, 2022[140])	**18**	*Act transposes the AVMSD.* Video sharing platform providers must take appropriate measures to protect minors from content that may disturb their "physical, psychological or moral development", ensuring that such content is providing in a way that minors cannot see or hear it. Content that contains **pornography** (or gross unjustified violence), can only be provided where technical measures are taken to prevent minor's access (at §48, 62). Appropriate measures for this purpose include the "establishment and operation of a system to verify the age of users" (at §49(1)(i)). The law defines a **minor** as a person younger than 18 years of age (at §62). **Video sharing platform** is as defined in the AVMSD, but the law specifies that it applies to those established in the Slovak Republic (at §7).	The law does not prescribe any particular age assurance method. The law does note (at §49(2)) that such a measure must be feasible and appropriate, taking into consideration: • the nature of the content provided; • any damage that the content may cause; • the groups of persons to be protected; • rights and legitimate interests, including those of the video sharing platform provider and the users who uploaded or created the content; and • the general public interest. The law further notes that any measures taken must not "lead to ex ante control measures or to content filtering "that is not otherwise covered in law (at §49(3)), and that the personal data of minors collected or otherwise obtained for assuring age must not be processed for commercial purposes (at §49(4)).	Rada pre vysielanie a retransmisiu
Slovenia*	Zakon o avdiovizualnih medijskih storitvah (ZAvMS) (Act on Audiovisual Media Services) (Government of Slovenia, 2011[141])	**18**	*Act transposes the AVMSD.* Video sharing platform providers must take appropriate measures to protect children from "programs, videos and audiovisual commercial messages that could harm their physical, mental or moral development" (at art. 38b (1)). Content that could harm the physical, mental or moral development of children, is defined as including **pornography** (as well as gratuitous violence) (at art.14(1)). Appropriate measures include "establishment and management of a system for checking the age of users" (at art 38b(7)). The law does not define **child**, but Slovenia's General Child Protection in Audiovisual Media Services Act defines a child as a person who has not reached 18 (Government of Slovenia, 2022[142]).	The law does not prescribe any particular age assurance method. The law further notes that any measures taken must not to measures of "prior control or filtering of content" that is not otherwise covered in law (at art 38b(9)), and that any personal data collected or otherwise obtained for assuring age must only be processed for an age assurance purpose (at art 38b(8)).	Agencija za komunikacijska omrežja in storitve Republike Slovenije (AKOS)

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
Spain*	General de Comunicación Audiovisual (General Law on Audiovisual Communication) (Government of Spain, 2022[143])	**18**	*Act transposes the AVMSD.* The law requires that providers of video sharing services take measures to protect "minors from programs, user-generated videos and audiovisual commercial communications that may harm their physical, mental or moral development" (at art. 88). Measures are defined to include establishing and operating "age verification systems for users with respect to content that may harm the physical, mental or moral development of minors, which in any case prevent their access to the most harmful audiovisual content, such as gratuitous violence or **pornography**" (at art 89) (emphasis added). Minor is not defined in the law, but Spain's Civil Code (Government of Spain, 1889[144]) defines the age of majority as 18 (at art 315).	The law does not prescribe a particular age assurance method. The law does provide that minor's personal collected or otherwise generated by the video sharing service for the purpose of *inter* alia age assurance may not be processed for commercial purposes (at art. 90).	Comisión Nacional de los Mercados y de la Competencia
Sweden*	Radio and Television Act (2010) (Government of Sweden, 2010[147])	**18**	*Act transposes the AVMSD.* The Act requires that "a video-sharing platform provider shall **take appropriate measures** to ensure that user generated videos, television programmes and audiovisual commercial communications that contain detailed depictions of realistic violence or **pornographic images** are not made available in such a manner that presents a significant risk that children will see them, unless this is justified for some special reason." (at ch 9a, s1) (emphasis added). The law does not specify if appropriate measures include age assurance. The law does not explicitly define **child**, but Swedish law considers everyone under 18 to be a child (migrationsverket, 2024[148]).	Unclear, the law does provide that "personal data collected or otherwise generated by video-sharing platform providers in order to fulfil the requirement for (appropriate) measures (…) may not be processed for commercial purposes".	Mediemyndigheten
Switzerland	Criminal Code (Government of Switzerland,	**16**	There is no law dealing with the distribution of pornography online. The Criminal Code (at art. 197) prohibits offering, showing, passing to, or making accessible to persons under 16,	N/a	Federal Office of Justice

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
	1937[194])		pornographic documents, sound or visual recordings, or depictions.		
Türkiye	Türk Ceza Kanunu (Penal Code) (Government of Türkiye, 2004[195]) Law No. 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed through Such Publications (Government of Türkiye, 2007[196])	**18**	The Penal Code (at art. 226) prohibits (including via the Internet): • giving, showing, reading to, or allowing a child to read products containing obscene images, texts or words; and • showing, displaying, reading, having read, telling or making others say their content in places where children can enter or see it, or in public. Obscene images are not further defined. Child is defined to mean a person who has not yet reached the age of 18 (at art. 6). Law No. 5651, while not including an age assurance provision, does enable the blocking of access to websites hosting pornographic or obscene content.	N/a	Ministry of Justice Information and Communications Technology Authority (BTK)
United Kingdom	Online Safety Act (Government of the United Kingdom, 2023[18])	**18**	The Online Safety Act (OSA) imposes specific duties on service providers regulated by the Act. These duties *inter alia* seek to ensure that children enjoy a higher standard of protection than adults (s1(3)(i)). A **child** is defined as a person under the age of 18 (s236). Regulated service providers are: • **user-to-user** services, (those that host user generated content), and have a link to the United Kingdom; • **search services** (an Internet service that is, or includes, a search engine), and have a link to the United Kingdom; and • all **providers of pornographic content**, noting that there is no need for a link to the United Kingdom, but that services which provide pornographic content consisting only of text, or text accompanied by a non-pornographic GIF or emoji are excluded (see s79(1)-(4)). (see Table A A.1 for further details on the provisions relevant to user-to-user and search services)	The Act provides that when a service is required to use age verification or age estimation, it must be of such a kind and used in such a way that renders it highly effective at correctly determining whether or not a particular user is a child (s12(6)), and s81(3)). The Act specifies that self-declaration alone is not to be regarded as age verification or age estimation (at s230). Pornographic providers are required to: • keep a record of the kinds of age verification / age estimation used, as well as how they are used (s81(4)(a)); • the way in which the provider has considered their obligations under any United Kingdom privacy law, when deciding which methods to use and how to use them (s81(4)(b)); and • summarise this written record in a publicly available statement. The Act instructs Ofcom to provide guidance to pornography providers as to how to comply with the above obligations (s82), setting out examples of: • the kinds and uses of age assurance that are (or are not) highly	Ofcom

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
			Providers of **pornographic content** have a duty to ensure, by way of age verification / age estimation (or both) that children are not usually able to encounter regulated pornographic content on their service (s81(2).	effective at determining age; • ways in which a provider can protect a user's privacy; • principles Ofcom proposed to apply in assessing compliance with the duties under the Act (at s81), and examples of what would be considered non-compliance. In setting this guidance Ofcom must have regard to (at s82(3): • the principle that age assurance should be easy to use; • the principle that age assurance should work effectively for all users regardless of their characteristics, or whether they are members of a certain group; • the principle of interoperability between different kinds of age assurance. In January 2025, Ofcom published "Guidance on highly effective age assurance and other part 5 duties" (Ofcom, 2025[197]). This guidance (at section 4) sets out "a non-exhaustive list of kinds of age assurance that could be highly effective at correctly determining whether or not a user is a child, as well as setting out some examples of methods that (Ofcom) consider are not capable of doing this". The guidance states that the list is "non-exhaustive" and intended to be future proof and technology neutral. It specifies that highly effective age assurance must be: i) technically accurate; ii) robust iii) reliable; and iv) fair; and specifies the following examples: • open banking • photo-ID matching • facial age estimation • mobile network operator age check • credit card • digital identity wallets. It specifies the following as <u>not</u> highly effective: • self-declaration	

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
				• debit, solo, or electron cards • other payment methods which do not require the user to be over 18 • general contractual restrictions on the use of the service by children	
United States *(Federal)*	18. US Code, Chapter 71 (Government of the United States, 1948[198])	**16**	There is not a federal US law dealing with the distribution of pornography online. The US Code does prohibit the "transfer of obscene materials to minors" using "the mail or any facility or means of interstate of foreign commerce", defining a minor as an individual under the age of 16 years (at §1470).	N/a	Department of Justice
United States *(Alabama)*	House Bill 164 (Alabama State Legislature, 2024[199])	**18**	Law aim to prevent minor's online exposure to pornography. Definitions: **Adult website** is a "website, application or digital or virtual platform that uses the Internet to facilitate the dissemination of pictures, videos, or other content, a substantial portion of which is sexual material harmful to minors". **Material harmful to minors** is as defined in Alabama's Code at s13A-12-200.1 (Alabama State Legislature, 1975[200]), which is: i) material that the "average person, applying contemporary community standards, would find (…) taken as a whole, appeals to the prurient interest of minors; ii) "depicts or describes [body parts / sexual acts] in a way which is patently offensive to prevailing standards in the adult community with respect to what is suitable for minors"; and the material taken as a whole lacks literary, artistic, political or scientific value for minors. **Minor** is an individual under 18 years of age. A **substantial portion** of content is more than $33^{1/3}$ percent.	Any commercial entity that "knowingly and intentionally publishes or distributes sexual material harmful to minors through an adult website" is required to use a "reasonable age-verification method" to provide "reasonable assurance" that the material is not accessible to individuals under 18 years of age. The law defines a "reasonable age-verification method" as "any commercially available software, application, program or methodology that, when enabled, provides reasonable assurances that any individual accessing certain published material is 18 years or older". The law further provides that neither the commercial entity offering the adult website service, nor a third party can retain any personally identifying information of the person whose age has been assured after they have been granted access to the service.	Establishes a private right of action. Upon filing any action, the plaintiff must notify the Attorney-General. If an action succeeds the Attorney-General can levy a civil penalty
United States *(Arkansas)*	The Protection of Minors from Distribution of Harmful Material Act (Senate Bill 66)	**18**	Law aims to prevent minor's online exposure to material harmful to them. Definitions:	Commercial entities are required to use a "reasonable age verification method before allowing access to a website that contains a substantial portion of material that is harmful to minors".	Establishes a private right of action.

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
	(Arkansas State Senate, 2023[201])		**Commercial entity** is a "corporation, limited liability company, partnership, limited partnership, sole proprietorship, or other legally recognized entity." It includes third-party vendors. **Material harmful to minors** is: i) "Any material that the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, prurient interest"; and ii) "material that exploits, is devoted to, or principally consists of descriptions of actual, simulated, or animated displays or depictions of [body parts / sexual acts], in a manner patently offensive with respect to minors"; and the material taken as a whole lacks literary, artistic, political or scientific value. **Minor** is an individual under 18 years of age. A **substantial portion** of content is more than 33.33 percent.	Reasonable age verification is defined as confirming "that a person seeking to access published material that may have a substantial portion of material that is harmful to minors is at least 18 years of age" Reasonable age verification methods include: a digitized identification card; government-issued identification; or "any commercially reasonable age verification method that holds an Identity Assurance Level 2 (IAL2)".	
United States *(Florida)*	An act relating to online protections for minors (House Bill 3) (Florida State Legislature, 2024[164])	**18**	Law aims to prevent minor's online access to material harmful to them. Definitions **Commercial entity** is a "corporation, limited liability company, a partnership, a limited partnership, a sole proprietorship, and any other legally recognized entity". **Material harmful to minors** is any material that: i) "the average person applying contemporary community standards would find, taken as a whole, appeals to the prurient interest"; ii) "depicts or describes, in a patently offensive way, sexual conduct as described in (Florida's obscenity law)"; and the material taken as a whole lacks serious literary, artistic, political or scientific value for minors. **Minor** is not expressly defined, but Florida's obscenity laws relevant to accessing pornography define a minor as any person	A commercial entity that "knowingly and intentionally publishes or distributes material harmful to minors on a website or application" that contains a "substantial portion of material harmful to minors" must "use either anonymous age verification or standard age verification to verify that the age of a person attempting to access the material is (over 18) and prevent access to the material to a person (under 18). The commercial entity must offer both an anonymous and standard age verification method to the user attempting to access the website/application. **Anonymous age verification** is defined as "a commercially reasonable method used by a government agency or business for the purpose of age verification which is conducted by a non-governmental independent third-party organized under the laws of the United States which: a) has it principle place of business in a state of the United States and b) is not owned or controlled by a company formed in a foreign country, a government of a foreign	Department of Legal Affairs (actions to be brought under the Florida Deceptive and Unfair Trade Practices Act) Law also establishes a private right of action

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
			younger than 18 years of age (Florida State Legislature, 2024[202]). **Substantial portion** means more that 33.3% of total material on a website or application.	country, or any other entity formed in a foreign country". Third party providers must protect and keep anonymous any personally identifying information, and not retain after assuring age. **Standard age verification** is defined as "any commercially reasonable method of age verification approved by the commercial entity"	
United States *(Georgia)*	Protecting Georgia's Children on Social Media Act of 2024 (Senate Bill 351) (Georgia State Legislature, 2024[165])	**18**	Law aims to prevent minors accessing material harmful to them. Definitions **Commercial entity** is a "corporation, limited liability company, partnership, limited partnership, sole proprietorship, or other legally recognized entity". **Material harmful to minors** includes: i) "Any material that the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, prurient interest"; ii) "material that exploits, are devoted to, or principally consists of descriptions of actual, simulated, or animated displays or depictions of [body parts / sexual acts], in a manner patently offensive with respect to minors"; and the material taken as a whole lacks serious literary, artistic, political or scientific value for minors. **Minor** is "any individual under the age of 18 years". **Substantial portion** means more than 33.3% of total material on a public website.	Commercial entities are required to use a "reasonable age verification method" before "allowing access to a public website that contains a substantial portion of material that is harmful to minors". Reasonable age verification is defined as confirming "that a person seeking to access published material that may have a substantial portion of material that is harmful to minors is at least 18 years of age". "Reasonable age verification methods" include (but are not limited to): a digitized identification card; government-issued identification; or "any commercially reasonable age verification method that meets or exceeds an Identity Assurance Level 2 standard, as defined by (NIST)". The law further provides that neither the commercial entity, nor a third party can retain any personally identifying information of the person whose age has been assured after they have been granted access to the material.	Attorney General (Civil penalties)
United States *(Idaho)*	Liability for Publishers and Distributors of Material Harmful to Minors on the Internet (House Bill 498)	**18**	Law aims to prevent minors access and exposure to pornography. Definitions **Commercial entity** is a "corporation, a limited liability company,	Commercial entities will face liability if they "knowingly and intentionally publish material harmful to minors on the internet from a website that contains a substantial portion of such material" and do not "perform reasonable age verification to verify the age of individuals attempting to access the material, or after verifying the age of the individual, provides a minor access to the material"	Attorney General (Civil penalties). Law also establishes a private right of action

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
	(Idaho State Legislature, 2024[203])		a partnership, a limited partnership, a sole proprietorship, or another legally recognized business entity". **Material harmful to minors** includes: i) "material that the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, prurient interest"; ii) "material that is devoted to or principally consists of descriptions of actual, simulated, or animated displays or depictions of [body parts / sexual acts], in a manner patently offensive with respect to minors"; and the material taken as a whole lacks serious literary, artistic, political or scientific value for minors. **Minor** is "any person under the age of 18 years". **Substantial portion** means more than 1/3rd of total material on a website.	"Reasonable age verification methods" include verifying that the person seeking access is over 18 by that person: • providing a digitised identification card; or • using a "commercial age verification system that verifies age" by: government ID; or public or private transactional data. The law further provides that neither the commercial entity, nor a third party can retain any identifying information of the person whose age has been assured.	
United States *(Indiana)*	Age verification for material harmful to minors (Senate Bill 17) (Indiana State Legislature, 2024[204])	**18**	Law aims to prevent minors accessing adult-oriented websites. Definitions: **Adult oriented website** is a "publicly accessible website that publishes material harmful to minors, if at least 1/3rd of the images and videos published on the website depict material harmful to minors". **Material harmful to minors** is as defined in Indiana's Criminal Law and Procedure Code at IC-35-49-2-2. (Indiana State Legislature, 1983[205]), which is "matter or performance" that: i) " describes or represents, in any form, nudity, sexual conduct, sexual excitement, or sado-masochistic abuse"; ii) considered as a whole, appeals to the prurient interest in sex of minors; iii) "is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable matter for or performance before minors"; and considered as a whole "lacks serious literary, artistic, political, or scientific value for minors".	Operators of adult oriented websites, may not "knowingly and intentionally publish an adult oriented website" unless the operator "uses a reasonable age verification method to prevent a minor" accessing the site. "Reasonable age verification methods" include verifying that the person seeking access is not a minor, via: • digitised ID (as defined under "mobile credential" in Indiana's Motor Vehicles Code (Indiana State Legisature, 2020[206])); or • "an independent third party age verification service that compares the identifying information entered by the individual who is seeking access with material that is available from a commercially available data base, or an aggregate of data bases, that is regularly used by government agencies and businesses for the purpose of age and identity verification; or • "any commercially reasonable method that relies on public or private transactional data to verify the age of the individual attempting to access the material".	Attorney General (Civil penalties). Law also establishes a private right of action

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
			Minor is a "person less than 18 years of age".	The law further provides that neither the commercial entity, nor a third party can retain any identifying information of the person whose age has been assured.	
United States *(Kansas)*	Senate Bill 394 (Kansas State Legislature, 2024[207])	**18**	Law aims to prevent minors accessing material harmful to them. Definitions: **Commercial entity** is a "corporation, a partnership, limited liability company, limited liability partnership, limited partnership, a sole proprietorship, or any other for profit organization". **Material harmful to minors** is as defined in K.S.A. 21-6402 (Kansas State Legislature, 2011[208]), which are material or performances that The average adult person applying contemporary community standards would; i) find "has a predominant tendency to appeal to a prurient interest in sex to minors''; ii) depicts or describes nudity, sexual conduct, sexual excitement or sadomasochistic abuse in a manner that is patently offensive to prevailing standards in the adult community with respect to what is suitable for minors; and "a reasonable person would find that the material or performance lacks serious literary, scientific, educational, artistic or political value for minors". The law does not expressly define **minor** but refers to persons "18 years or older".	Commercial entities that "knowingly shares or distributes material that is harmful to minors on a website" with the material appearing on "25% or more of the webpages viewed on such website in any calendar month", or that knowingly hosts such a website, are required to verify that any person attempting to access the website (resident in or located in Kansas at the time of attempted access) must verify that that person is 18 years or older. Age verification is to be "conducted through the use of: (1) A commercially available database that is regularly used by businesses or governmental entities for the purpose of age and identity verification; or (2) any other commercially reasonable method of age and identity verification." The law further provides that neither the commercial entity, nor a third party can retain any identifying information of the person whose age has been assured after access to the website.	Attorney General (Civil penalty) Law also establishes a private right of action.
United States *(Kentucky)*	An Act relating to the protection of children (House Bill 278) (Kentucky State Legislature, 2024[209])	**18**	Law aims to prevent minors accessing material harmful to them. Definitions: **Covered platforms** are entities that are: i) a website; and ii) in the regular course or trade or business of creating, hosting, or making available content that meets the definition of matter harmful to minors. Regardless of whether or not creating, hosting or making available this content is the principal business of the entity, its sole source of income, or if the entity actually earns a	Covered platforms "that knowingly and intentionally publishes or distributes material on the internet, more than one-third (1/3) of which is matter harmful to minors and fails to perform age verification, either by itself or through a third party, of individuals attempting to access the matter" will face liability. "Age verification" is defined as "verifying that the person seeking access to the matter is 18 years old or older through any of the following methods": • state issued ID; • ID issued by any agency of the United States government that	Establishes (exclusively) a private right of action.

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
			profit on these activities. **Matter harmful to minors** means: i) "any matter that the average person, applying contemporary community standards, and taking the material as a whole with respect to minors, would find is designed to appeal to, or pander to, the prurient interest"; ii) "any matter that exploits, is devoted to or principally consists of descriptions of actual, simulated, or animated displays or depictions of [body parts / sexual acts], in a manner patently offensive with respect to minors"; and the matter taken as a whole lacks serious literary, artistic, political or scientific value for minors. **Minor** is "any person under the age of 18 years".	establishes age; or • "Any commercially reasonable method of identification that relies on public or private transactional data to verify that the person" attempting to access is 18 or older. The law further provides that neither the covered platform, nor a third party can retain any identifying information of the person whose age has been assured after access to the website.	
United States *(Louisiana)*	Liability for publishers and distributors of material harmful to minors (Act No. 440) (Lousiana State Legislature, 2023[210])	**`18**	Law aims to prevent distribution to minors of material harmful to them, and limit minors exposure to pornography. Definitions: **Commercial entity** includes "corporations, limited liability companies, partnerships, limited partnerships, sole proprietorships, or other legally recognized entities." **Material harmful to minors** is all of: i) "any material that the average person, applying contemporary community standards would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest"; ii) any material that "exploits, is devoted to, or principally consists of descriptions of actual, simulated, or animated displays or depictions of [body parts / sexual acts], in a manner patently offensive with respect to minors"; iii) the "material taken as a whole lacks serious literary, artistic, political or scientific value for minors". **Minor** is "any person under the age of 18 years". **Substantial portion** is more than $33^{1/3}$ percent of total material.	Commercial entities will face private liability if they knowingly and intentionally publish or distribute "material harmful to minors on the internet from a website that contains a substantial portion of such material" and fail to "perform reasonable age verification methods to verify the age of individuals attempting to access the material". Reasonable age verification methods" include verifying that the person seeking access is over 18 by that person: • providing a digitised identification card; or • complying with a "commercial age verification system that verifies age" by: government issued ID; or relies on public or private transactional data. The law further provides that neither the commercial entity, nor a third party can retain any identifying information of the person whose age has been assured after access to the website.	Establishes a private right of action.

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
United States *(Louisiana)*	Act no. 216 (House Bill 77) (Louisiana State Legislature, 2023[211])	**18**	Law aims to prevent distribution to minors of material harmful to them, and limit minors exposure to pornography. Definitions: **Commercial entity** includes "corporations, limited liability companies, partnerships, limited partnerships, sole proprietorships, or other legally recognized entities." **Material harmful to minors** is all of: i) "any material that the average person, applying contemporary community standards would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest"; ii) any material that "exploits, is devoted to, or principally consists of descriptions of actual, simulated, or animated displays or depictions of [body parts / sexual acts], in a manner patently offensive with respect to minors"; iii) the "material taken as a whole lacks serious literary, artistic, political or scientific value for minors". **Minor** is "any person under the age of 18 years". **Substantial portion** is more than $33^{1/3}$ percent of total material.	Commercial entities will face civil penalties if they knowingly and intentionally publish or distribute "material harmful to minors on the internet from a website that contains a substantial portion of such material" and fail to "perform reasonable age verification methods to verify the age of individuals attempting to access the material". Reasonable age verification methods" include verifying that the person seeking access is over 18 by that person: • providing a digitised identification card; or • complying with a "commercial age verification system that verifies age" by: government issued ID; or relies on public or private transactional data.	Attorney General (civil penalty)
United States *(Mississippi)*	Senate Bill 2346 (Mississippi State Legislature, 2023[212])	**18**	Regulates children's exposure to pornographic media. Definitions: **Commercial entity** includes "corporations, limited liability companies, partnerships, limited partnerships, sole proprietorships, or other legally recognized entities." **Material harmful to minors** is all of: i) "any material that the average person, applying contemporary community standards would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest"; ii) any material that "exploits, is devoted to, or principally consists of descriptions of actual, simulated, or animated displays or depictions of [body parts / sexual acts], in a manner patently offensive with respect to minors"; iii) the	Commercial entities "that knowingly and intentionally publishes or distributes material harmful to minors on the internet from a website that contains a substantial portion of such material" and fail to "perform reasonable age verification methods to verify the age of the individuals attempting access" will face liability. Reasonable age verification methods" include verifying that the person seeking access is over 18 by that person: • providing a digitised identification card; or • complying with a "commercial age verification system that verifies age" by: government issued ID; or "any commercially reasonable method that relies on public or private transactional data". The law further provides that neither the commercial entity, nor a	Establishes a private right of action.

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
			"material taken as a whole lacks serious literary, artistic, political or scientific value for minors". **Minor** is "any person under the age of 18 years". **Substantial portion** is more than $33^{1/3}$ percent of total material.	third party can retain any identifying information of the person whose age has been assured after access to the website.	
United States *(Montana)*	Senate Bill 544 (Montana State Legislature, 2024[213])	**18**	Law aims to prevent distribution to minors of material harmful to them, and limit minors exposure to pornography. Definitions: **Commercial entity** includes "corporations, limited liability companies, partnerships, limited partnerships, sole proprietorships, or other legally recognized entities" **Material harmful to minors** is "all of the following: (i) any material that the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest; (b) any of [specified body parts / sexual acts] that exploits, is devoted to, or principally consists of descriptions of actual, simulated, or animated display or depiction of any of the following, in a manner patently offensive with respect to minors; and (c) the material taken as a whole lacks serious literary, artistic, political, or scientific value for minors". **Minor** is "any person under 18 years of age". **Substantial portion** is "more than $33^{1/3}$% of total material on a website, which meets the definition of "material harmful to minors"".	Commercial entities that "knowingly and intentionally publishes or distributes material harmful to minors on the Internet from a website that contains a substantial portion of material" will face liability "if the entity fails to perform reasonable age verification methods to verify the age the individuals attempting to access the material". ""Reasonable age verification methods" include verifying that the person seeking to access the material is 18 years of age or older by using any of the following methods: • providing a digitised identification card; or • complying with a "commercial age verification system that verifies in one or more of the following ways" by: government issued ID; or "any commercially reasonable method that relies on public or private transactional data to verify the age of the person attempting to access the information is at least 18 years of age or older". The law further provides that neither the commercial entity, nor a third party can retain any identifying information of the individual whose age has been assured after access to the material.	Establishes a private right of action
United States *(Nebraska)*	Online Age Verification Liability Act (LB 1092) (Nebraska State Legislature,	**18**	Law aims to prevent distribution to minors of material harmful to them. Definitions: **Commercial entity** includes "a corporation, limited liability	Commercial entities will face liability if they "knowingly and intentionally publish or distribute material harmful to minors on the Internet on a website that contains a substantial portion of such material unless the entity uses a reasonable age verification method to verify the age of an individual attempting to access the material".	Establishes a private right of action

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
	2024[214])		company, partnership, limited partnership, sole proprietorship, or other legally recognized entity" **Material harmful to minors** is "any material to which all of the following apply: (a) The average person, applying contemporary community standards, would find, taking the material as a whole and with respect to its consumption by minors, that such material is designed to appeal to or pander to the prurient interest; (b) The material is patently offensive to prevailing standards in the adult community as a whole with respect to its consumption by minors; and (c) The material taken as a whole lacks serious literary, artistic, political, or scientific value for minors" **Minor** is "any person under 18 years of age". **Substantial portion** is more than one-third of total material on the website	A "reasonable age verification method" is a "process to verify that the person attempting to access the material is at least eighteen years of age or older" through the use of: • a digitised identification card; • a government-issued identification; • a "financial document or other document that is a reliable proxy for age", or • "any commercially reasonable method that relies on public or private transactional data to verify the [persons] age". The law further provides that neither the commercial entity, nor a third party can retain any identifying information of the person whose age has been assured after access to the material.	
United States *(North Carolina)*	Pornography Age Verification Enforcement (PAVE) Act (House Bill 8) (North Carolina State Legislature, 2023[215])	**18**	Law aims to prevent distribution to minors of material harmful to them. Definitions: **Commercial entities** are "corporations, limited liability companies, partnerships, limited partnerships, sole proprietorships, or other legally recognized entities". **Material harmful to minors** is as defined in North Carolina's General Statute at G.S. 14-190.13 (North Carolina State Legislature, 2023[216]), which is "material or performance that depicts sexually explicit nudity or sexual activity and that, taken as a whole, has the following characteristics: a) The average adult person applying contemporary community standards would find that the material or performance has a predominant tendency to appeal to a prurient interest of minors in sex; and b) The average adult person applying contemporary community standards would find that the depiction of sexually explicit nudity or sexual activity in the material or performance is patently	Commercial entities that "knowingly and intentionally publishes or distributes material harmful to minors on the internet from a website that contains a substantial portion of such material" are required to use age verification. Age verification is to be through "use of (i) a commercially available database that is regularly used by businesses or governmental entities for the purpose of age and identity verification, or (ii) another commercially reasonable method of age and identity verification, verify the age of the individuals attempting to access the material". The law further provides that neither the commercial entity, nor a third party can retain any identifying information of the person whose age has been assured after access to the material.	Establishes a private right of action

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
			offensive to prevailing standards in the adult community concerning what is suitable for minors; and c). The material or performance lacks serious literary, artistic, political, or scientific value for minors". **Minor** is not expressly defined, but North Carolina's General Statute at G.S. 14-190.13 (North Carolina State Legislature, 2023[216])defines a minor as "An individual who is less than 18 years old and is not married or judicially emancipated". **Substantial portion** is more than $33^{1/3}$ % of total material on a website.		
United States *(Oklahoma)*	Senate Bill 1959 (Oklahoma State Legislature, 2024[217])		Law aims to prevent distribution to minors of material harmful to them. Definitions: **Commercial entity** means "a corporation, limited liability company, partnership, limited partnership, sole proprietorship, or other legally recognized entity". **Harmful to minors** is as defined in the Oklahoma Statutes (Title 21) at ss1040.75-77 (Oklahoma State Legislature, 2024[218]), which is, A) "any description, exhibition, presentation or representation, in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse when the material or performance, taken as a whole, has the following characteristics: (1) the average person eighteen (18) years of age or older applying contemporary community standards would find that the material or performance has a predominant tendency to appeal to a prurient interest in sex to minors, and (2) the average person eighteen (18) years of age or older applying contemporary community standards would find that the material or performance depicts or describes nudity, sexual conduct, sexual excitement or sadomasochistic abuse in a manner that is	Commercial entities that "knowingly and intentionally publishes or distributes material harmful to minors on the Internet from a website that contains a substantial portion of such material" are required to provide "Internet service subscribers and cellular service subscribers the opportunity, before any individual using such services may access the material, to request that access to the material by subscription service be denied". Upon such a request, commercial entities must "without charge, block access to its website on any device seeking to access its website using the subscriber's Internet service or cellular service subscription so that a minor does not receive material harmful to minors via that subscription". Relevant commercial entities that fail to block access will face liability. It is a defense to liability if the commercial entity "performs reasonable age verification methods to verify that the individual attempting to access the material from its website is not a minor", "Reasonable age verification methods" means to verify the person seeking access is 18 or older through the following methods: • use of a digitized identification card; • "verification through an independent, third-party age verification service that compares the personal information	Attorney General (Injunctive relief) Law also establishes a private right of action.

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
			patently offensive to prevailing standards in the adult community with respect to what is suitable for minors, and (3) the material or performance lacks serious literary, scientific, medical, artistic, or political value for minors; or B) any description, exhibition, presentation or representation, in whatever form, of inappropriate violence". **Minor** is "any person 18 years of age or younger" **Substantial portion** is more than a third of the total material available on the website.	entered by the individual who is seeking access to the material that is available from a commercially available database, or aggregate of databases, that is regularly used by government agencies and businesses for purpose of age and identity verification"; or • any commercially reasonable method that relies on public or private transactional data. The law further provides that neither the commercial entity, nor a third party can retain any identifying information of the person whose age has been assured after access to the material.	
United States *(South Carolina)*	House Bill 3424 (South Carolina State Legislature, 2024[219])		Law aims to prevent minors access to pornography. Definitions: **Commercial entity** "includes corporations, limited liability companies, partnerships, limited partnerships, sole proprietorships, or other legally recognized entities". **Material harmful to minors** is as defined in the South Carolina Code of Laws (at 16-15-375) (South Carolina State Legislature, 1987[220]), which is: "that quality of any material or performance that depicts sexually explicit nudity or sexual activity and that, taken as a whole, has the following characteristics: (a) the average adult person applying contemporary community standards would find that the material or performance has a predominant tendency to appeal to a prurient interest of minors in sex; and (b) the average adult person applying contemporary community standards would find that the depiction of sexually explicit nudity or sexual activity in the material or performance is patently offensive to prevailing standards in the adult community concerning what is suitable for minors; and (c) to a reasonable person, the material or performance taken as a whole lacks serious literary, artistic, political, or scientific value for minors". **Material** means "pictures, drawings, video recordings, films, digital electronic files, or other visual depictions or representations but not material consisting entirely of written	From 1 January 2025, commercial entities that "knowingly and intentionally publishes or distributes material harmful to minors on the Internet from a website that contains a substantial portion of such material" will face liability if "if the entity fails to perform reasonable age verification methods to verify the age of an individual attempting to access the material". "Reasonable age verification methods" means "verifying that the person seeking to access the material is eighteen years old or older by using any of the following methods": • digitized identification; • "verification through an independent, third-party age verification service that compares the personal information entered by the individual who is seeking access to the material that is available from a commercially available database, or aggregate of databases, that is regularly used by government agencies and businesses for the purpose of age and identity verification"; or • any commercially reasonable method that relies on public or private transactional data. The law further provides that neither the commercial entity, nor a third party can retain any identifying information of the person whose age has been assured after access to the material.	Establishes a private right of action Attorney General may also seek injunctive relief

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
			words". **Minor** is as defined in the South Carolina Code of Laws (at 16-15-375) (South Carolina State Legislature, 1987[220]), which is "an individual who is less than eighteen years old". **Substantial portion** means more that $33^{1/3}$ % of total material on a website.		
United States *(South Dakota)*	An Act to require age verification by websites containing material that is harmful to minors, and to provide a penalty therefor (House Bill 1053) (South Dakota State Legislature, 2025[221])	**18**	Law aims to prevent minors access to pornography. Definitions: **Covered platform** is a website for which in the regular course of its trade or business creates, hosts, or makes available material that is harmful to minors; **Material harmful to minors** is material that includes "any description or representation, in whatever form, of nudity, sexual conduct, sexual excitement, or sado-masochistic abuse, if it: (a) predominantly appeals to the prurient, shameful, or morbid interest of minors; and (b) Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material for minors; and (c) Is without serious literary, artistic, political, or scientific value. **Minor** is any person less than eighteen years of age.	Covered platforms must implement reasonable age verification on to verify the age of any individual who attempts to access material that is harmful to minors, and to prevent a minor's access to that material. "Reasonable age verification," is defined as any method by which a covered platform confirms that an individual attempting to access material that is harmful to minors is at least eighteen years of age by verifying: • A state-issued driver license or non-driver identification card; • The individual's bank account information; • A debit or credit card from the individual that requires the individual in ownership of the card to be at least eighteen years of age; or • Any other method or document that reliably and accurately indicates if a user of a covered platform is a minor and prevents a minor from accessing the content of a covered platform;	Attorney General (criminal and civil penalty)
United States *(Tennessee)*	Protect Tennessee Minors Act (Senate Bill 1792) (Tennessee State Legislature, 2024[222])	**18**	Law aims to prevent minors access to material harmful to them. Definitions: **Active user** is a "viewer of a website". **Age-verified session** is the "lesser of the session during which the active user's age was verified using a reasonable age-verification method or 60 minutes from the time the active user's age was verified". **Commercial entity** is "a corporation, limited liability company,	An individual or a commercial entity that publishes or distributes a website in Tennessee that contains a substantial portion of material harmful to minors, will face liability if they do not: • "verify, using a reasonable age-verification method, the age of each active user attempting to access its website; or • verify, using a reasonable age-verification method, the age of an active user attempting to access its website again after completion of an age-verified session". A "reasonable age-verification method" includes: • matching a photograph of the active user taken between an	Attorney General

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
			partnership, limited partnership, sole proprietorship, or other legally recognized entity". **Content harmful to minors** is "(i) text, audio, imagery, or video the average person, applying contemporary community standards and taking the material as a whole and with respect to minors of any age, would find sexually explicit and harmful or inappropriate for minors or designed to appeal to or pander to the prurient interest; or (ii) Text, audio, imagery, or video that exploits, is devoted to, or principally consists of an actual, simulated, or animated display or depiction of [specified body parts / sexual acts]; and when taken as a whole lacks serious literary, artistic, political, or scientific value for minors". **Minor** is a person under 18 years of age. **Substantial portion** is $33^{1/3}$ % or more of the total amount of data available on a website.	attempt to view the material and viewing the material "using the device by which the attempt to view" is made, to "the photograph on a valid form of identification issued by a state of the United States of America"; or • a commercially reasonable method relying on public or private transactional data. The law further provides that the website owner, commercial entity, or a third party cannot retain any identifying information of the active user after granting access to the material. The law does provide that anonymised age-verification data must be retained by the website, commercial entity or third party for at least 7 years.	
United States *(Texas)*	Securing Children Online through Parental Empowerment (SCOPE) Act (House Bill 18) (Texas State Legislature, 2023[169])	**18**	Aims to prevent minors access to material harmful to them. Definitions: **Digital service** is "a website, an application, a program, or software that collects or processes personal identifying information with Internet connectivity". **Digital service provider** is "a person who: (a) owns or operates a digital service; (b) determines the purpose of collecting and processing the personal identifying information of users of the digital service; and (c) determines the means used to collect and process the personal identifying information of users of the digital service". **Material harmful to minors** is as defined by Section 43.21, of the Texas Penal Code (Texas State Legislature, 1993[223]), which is "material or a performance that: (A) the average person, applying contemporary community standards, would find that	A digital service provider that "knowingly publishes or distributes material, more than one-third of which is harmful material or obscene (as defined by the Texas Penal Code) must use a commercially reasonable age verification method to verify that any person seeking to access content on or through the provider 's digital service is 18 years of age or older". The digital service provider must also not enter into any agreement with a person under 18 to access the service. The law does not provide further detail beyond "commercially reasonable age verification method".	Establishes a private right of action (declaratory or injunctive relief) to be brought exclusively by a parent or guardian.

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
			taken as a whole appeals to the prurient interest in sex; (B) depicts or describes: (i) patently offensive representations or descriptions of ultimate sexual acts, normal or perverted, actual or simulated, including sexual intercourse, sodomy, and sexual bestiality; or (ii) patently offensive representations or descriptions of masturbation, excretory functions, sadism, masochism, lewd exhibition of the genitals, the male or female genitals in a state of sexual stimulation or arousal, covered male genitals in a discernibly turgid state or a device designed and marketed as useful primarily for stimulation of the human genital organs; and (C) taken as a whole, lacks serious literary, artistic, political, and scientific value. **Minor** is a child younger than 18 who has not had "the disabilities of minority removed for general purposes".		
United States (*Utah*)	Online Pornography Viewing Age Requirements (Senate Bill 287) (Utah State Legislature, 2023[224])	**18**	Law aims to prevent minors access to material harmful to them. <u>Definitions:</u> **Commercial entity** includes "corporations, limited liability companies, partnerships, limited partnerships, sole proprietorships, or other legally recognized entities". **Material harmful to minors** is defined as all of: "(a) any material that the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest; (b) material that exploits, is devoted to, or principally consists of descriptions of actual, simulated, or animated display or depiction of [specified body parts / sexual acts] in a manner patently offensive with respect to minors; and (c) the material taken as a whole lacks serious literary, artistic, political, or scientific value for minors." **Minor** is any person under 18 years old. **Substantial portion** is more than $33^{1/3}$ % of total material on a	A commercial entity that "knowingly and intentionally publishes or distributes material harmful to minors on the Internet from a website that contains a substantial portion of such material shall be held liable if the entity fails to perform reasonable age verification methods to verify the age of an individual attempting to access the material". Reasonable age verification methods verify that the person seeking to access the material is 18 years old or older by using any of the following methods: • Digitised ID; • "verification through an independent, third-party age verification service that compares the personal information entered by the individual who is seeking access to the material that is available from a commercially available database, or aggregate of databases, that is regularly used by government agencies and businesses for the purpose of age and identity verification"; or • any commercially reasonable method that relies on public or private transactional data. The law further provides that neither the commercial entity, nor a	Establishes a private right of action

© OECD 2025

Country / Region	Law	Age Limit	Purpose / Scope of Law	Online Age Assurance Requirement	Administrator
			website.	third party can retain any identifying information of the person whose age has been assured after access to the material.	
United States *(Virginia)*	Senate Bill 1515 (Virginia State Legislature, 2023[225])	**18**	Law aims to prevent minors access to material harmful to them. Definitions: **Commercial entity** is not defined. **Material harmful to minors** means "any description or representation of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse when it (i) appeals to the prurient, shameful, or morbid interest of minors, (ii) is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material for minors, and (iii) is, when taken as a whole, lacking in serious literary, artistic, political, or scientific value for minors" The law does not expressly define **minor** but refers to persons "18 years or older".	Any commercial entity that "knowingly or intentionally publishes or distributes material harmful to minors on the Internet from a website that contains a substantial portion of such material" will face liability if they do not verify that any person attempting access is 18 years or older "through the use of (i) a commercially available database that is regularly used by businesses or governmental entities for the purpose of age and identity verification or (ii) another commercially reasonable method of age and identity verification." Methods of age assurances are not otherwise defined.	Establishes a private right of action
United States (*Wyoming*)	Age verification for websites with harmful material (HB0043) (Wyoming State Legislature, 2025[226])	**18**	Law aims to prevent minors access to material harmful to them. Definitions: **Covered platform** is an entity that operates a website that, in the regular course of business, creates, hosts or makes available content that is material harmful to minors, regardless of whether that entity earns a profit or if such material is the source of income or principal business of the entity. **Material harmful to minors** is any picture, image, graphic image file, film, videotape or other visual depiction that is obscene or is child pornography. **Minor** is a person who has not obtained the age of 18 years.	Covered platforms are required to perform reasonable age verification methods to verify the age of all persons accessing or attempting to access the material and shall prevent access by minors to the material. Reasonable age verification methods include: • a Wyoming driver's license or identification card • a valid United States passport or military card • a tribal identification card; • a driver's license or identification card issued by any state or outlying possession of the United States; • a credit card or debit card, except for cards that do not require the person in ownership of the credit card account to be 18 or older The law further provides that neither the covered platform, nor a third party can retain any identifying information of the person whose age has been assured after access to the material.	Establishes a private right of action

"*".: Denotes EU and EEA Member States that are subject to the provisions of the AVMSD

© OECD 2025

Annex D. Privacy and data protection legal frameworks

Table A D.1 sets out the legal regimes across the OECD for protecting children's data and privacy, and the provisions within those laws that either: i) establish specific protections for processing children's data and define an age limit for this purpose; or ii) set an age beyond which children are able to consent to the processing of their data. It also, where relevant, covers specific provisions relevant to targeted advertising.

A number of laws require parental consent to process the data of children not deemed to have the relevant capacity. For this reason, a column is included setting out where a requirement for parental consent is in place.

The column "age limit" in this table gives the age at which children are considered to have capacity to consent to the processing of their data. Where a country's law is indicated to have "no set age", this reflects laws that establish no precise age at which children are deemed to have capacity, but rather specify that capacity is determined on a case-by-case basis. Where the age limit is "not stated", this reflects laws with no requirement distinguishing children's data, or children's capacity to consent, from adults. Where there is a stated age for providing special protection of children's data that differs from the consent age limit, this is noted in the column "basis for age limit". For EU/EEA countries, unless specifically addressed in the country's law, this is noted just once against the row for the "European Union".

Table A D.1. Age-based protections and methods for enforcing them in privacy and data protection laws

Country / Region	Law	Age Limit	Basis for age limit	Age Assurance Requirement	Requirement for parental consent	Administrator
Australia	Privacy Act (Government of Australia, 1988[227])	**No set age**	Australia's Privacy Act protects the personal information of all individuals regardless of age. Children's data is not subject to special protection. An individual must have capacity to make their own privacy decisions, and for any consent to be valid. For individuals under	N/a	There is no express requirement for parental consent. The Australian Privacy Principles Guidelines set out that where an individual lacks capacity consent must obtained from a person acting on their behalf. This could be a parent or	Office of the Australian Information Commissioner (OAIC)

© OECD 2025

Country / Region	Law	Age Limit	Basis for age limit	Age Assurance Requirement	Requirement for parental consent	Administrator
			18, any organisation handling their data will need to determine on a case-by-case basis if the individual has capacity to consent. The Australian Privacy Principles guidelines notes: "As a general rule, an individual under the age of 18 will have capacity to consent if they have the maturity to understand what's being proposed. If they lack maturity it may be appropriate for a parent or guardian to consent on their behalf. If it is not practical for an organisation or agency to assess the capacity of individuals on a case-by-case basis, as a general rule, an organisation or agency may assume an **individual over the age of 15** has capacity, unless they're unsure" (emphasis added). If there is uncertainty the organisation should obtain consent from a parent (or other person acting on the child's behalf) (Office of the Australian Information Commissioner, 2022[228]).		guardian but could also be a person with enduring power of attorney or someone appointed under law. The guidance notes that the individual lacking capacity should "nevertheless be involved, as far as practicable, in any decision-making process". As well as being given by a person with capacity, consent must be: informed, voluntary, current and specific (Office of the Australian Information Commissioner, 2022[228]).	
Austria*	Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Datenschutzgesetz (Consolidated Federal Law for the Data Protection Act) (Government of Austria, 2024[229])	**14**	Austria is subject to the provisions of the GDPR. Pursuant to GDPR article 8, Austrian law specifies a minimum age of consent as follows: "When an information society service is offered directly to a child, consent to the processing of the child's personal data is lawful (…) if the child has reached the age of fourteen" (at art. 4(4)).	See under EU	See under EU	Datenschutzbehörde (DSB)
Belgium*	Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (Law on the protection of individuals with regard to the	**13**	Belgium is subject to the provisions of the GDPR. Pursuant to GDPR article 8, Belgian law specifies a minimum age of consent as follows: "In accordance with Article 8.1 of the Regulation, the processing of personal data relating to children in relation to the direct offering of	See under EU	See under EU	Data Protection Authority (APD/GBA)

© OECD 2025

Country / Region	Law	Age Limit	Basis for age limit	Age Assurance Requirement	Requirement for parental consent	Administrator
	processing of personal data) (Government of Belgium, 2018[230])		information society services to children is lawful when consent has been given by children aged 13 or over. Where this processing concerns personal data of a child under 13 years of age, it is only lawful if consent is given by the legal representative of that child" (at art 7).			
Canada	Personal Information Protection and Electronic Documents Act (PIPEDA) (Government of Canada, 2000[231])	**No set age**	Canada's Privacy Act protects the personal information of all individuals regardless of age. The Act does not specify that children's data is subject to special protection, however guidance from the Office of the Privacy Commissioner (OPC) notes that children's data should be treated with "particular sensitivity", and sets out a number of recommendations for businesses, including that they: • limit or avoid altogether the collection of children's data; • be careful about inadvertent collection of data; • communicate privacy policies in a manner understandable to children (or their parents); • make it clear who is agreeing to terms and conditions (i.e. child or parent); and • engage appropriate default privacy settings (Office of the Privacy Commissioner Canada, 2015[232]). The Act requires that consent to processing data must be "meaningful". For children, guidance from the OPC notes that as a general rule children under the **age of**		There is no express requirement for parental consent. For persons unable to provide meaningful consent, including children under 13, OPC guidance states that consent must be obtained from a parent or guardian (Office of the Privacy Commissioner Canada, 2021[233]).	Office of the Privacy Commissioner (OPC)

© OECD 2025

Country / Region	Law	Age Limit	Basis for age limit	Age Assurance Requirement	Requirement for parental consent	Administrator
			13 should be considered unable to give meaningful consent, and that they require a parent to consent on their behalf (Office of the Privacy Commissioner Canada, 2021[233]).			
Chile	Ley no. 19.628 sobre Protección de la Vida Privada (Law on the Protection of Private Life) (Government of Chile, 1999[234])	**Not stated**	Chile's law does not provide any specific protections for children's data, nor contain any express provisions on a child's capacity to consent to their data being processed.	N/a	N/a	Servicio Nacional del Consumidor (SERNAC)
Colombia	Ley no. 1581 of 2012 por la cual se dictan disposiciones generales para la protección de datos personales (General Data Protection Law) (Government of Colombia, 2012[235])	**18**	Colombia's law prohibits all processing of a child's or adolescent's data, except data of a "public nature" (at art. 7). While the law itself does not deal with parental consent, Decree 1377 of 2013, does provide for a parent or guardian to consent on a "child's or adolescent's" behalf (at art. 12) (Government of Colombia, 2013[236]). Colombia's data protection law does not define a minor, however under Colombia's Code on childhood and adolescence defines a child as a person aged between 0-12 years, and an adolescent as any person between 12 and 18 (at art 3) (Government of Colombia, 2006[178]). Therefore, the data protection provisions relevant to children apply to anyone under **18**.	N/a	The law does not set out how parental consent is to be obtained. Decree 1377 of 2013 (at art. 12), does provide that the consent must be in accordance with the child's fundamental rights, be in their best interests, and be given after the child has had an opportunity to be heard (as appropriate with regard to the child's level of maturity) (Government of Colombia, 2013[236]).	Superintendencia de Industria y Comercio (SIC)
Costa Rica	Ley de Protección de la Persona frente al tratamiento de sus datos personales (Nº 8968) (Law on the Protection of the Person	**Not stated**	Costa Rica's law does not provide specific protections for children's data. It does require consent for the processing of personal data, and refer to "representatives" providing consent, without specifying the circumstances in	N/a	The law does not set out how "representatives would provide consent, nor when such a representative would be required.	Agencia de Protección de Datos de los Habitantes (PRODHAB)

© OECD 2025

Country / Region	Law	Age Limit	Basis for age limit	Age Assurance Requirement	Requirement for parental consent	Administrator
	Regarding the Processing of their Personal Data) (Government of Costa Rica, 2011[237])		which a representative would be required (at art. 5).			
Czechia*	Zákon o ochraně osobních údajů (Act on the Protection of Personal Data) (Government of Czechia, 2019[238])	**15**	Czechia is subject to the provisions of the GDPR. Pursuant to GDPR article 8, Czechia law specifies a minimum age of consent as follows: "A child acquires the capacity to consent to the processing of personal data in connection with the offer of information society services directly to him upon reaching the age of fifteen" (at s7).	See under EU	See under EU	Personal Data Protection Office
Denmark*	Databeskyttelsesloven (Data Protection Act) (Government of Denmark, 2018[239])	**13**	Denmark is subject to the provisions of the GDPR. Pursuant to GDPR article 8, Danish law specifies that the processing of personal data for a child under 13 is only lawful if "consent is given or approved by the holder of parental authority over the child" (at § 6).	See under EU	See under EU	Datatilsynet
Estonia*	Isikuandmete kaitse seadus (Personal Data Protection Act) (Government of Estonia, 2018[240])	**13**	Estonia is subject to the provisions of the GDPR. Pursuant to GDPR article 8, Estonian law specifies that the processing of the child's personal data is permitted only if the child is at least 13 years old, and that "If the child is younger than 13 years old, the processing of personal data is permitted only in such a case and to such an extent that the legal representative of the child has given consent" (at § 8).	See under EU	See under EU	Andmekaitse Inspektsioon
European Union	*General Data Protection Regulation (GDPR)* (European Commission, 2016[241])	***13 – 16***	***Data processing:*** *The processing of a child's personal data on the basis of consent (see art. 6.1.a) is lawful only when a child is: a) at least 16 years old, or b) the person with parental responsibility for the child has provided consent. EU Member States may provide for a lower age of*	*N/a*	*The data controller must make reasonable efforts to verify that consent is given or authorised by the person with parental responsibility over the child.* *The GDPR does not prescribe any particular method of verifying parental*	*European Commission* *Member State supervisory authorities*

© OECD 2025

Country / Region	Law	Age Limit	Basis for age limit	Age Assurance Requirement	Requirement for parental consent	Administrator
			consent, provided the age is not below 13 years. (Art. 8). *Art 8 of the GDPR applies to "**Information Society Services**", which are defined as: "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".* ***Ensuring special protection of children's data:** Where children's data is processed, it merits special protection (Recital 38).* *In addition to the above provisions, the Digital Services Act (DSA)* (European Commission, 2022[35]) *at art 28 provides that "providers of online platform shall not present advertisements on their interface based on profiling as defined in [art. 4(4) of the GDPR] using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor".* *Art 4(4) of the GDPP defines **profiling** as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements"*		*consent but does note that data processors may take into "consideration available technology" in carrying this out.*	

© OECD 2025

Country / Region	Law	Age Limit	Basis for age limit	Age Assurance Requirement	Requirement for parental consent	Administrator
			Child *is not defined in the GDPR or the DSA, however the European Commission's Better Internet for Kids Policy defines children as individuals under 18 years* (European Commission, 2022[103]).			
Finland*	Tietosuojalaki (Data Protection Act) (Government of Finland, 2018[242])	**13**	Finland is subject to the provisions of the GDPR. Pursuant to GDPR article 8, Finnish law specifies a minimum age of consent as follows: "Where personal data are processed based on consent referred to in [the GDPR] and in connection with offering of information society services referred to in [the Finnish Act] directly to a child, the processing of the personal data of the child is lawful where the child is at least 13 years old." (at s5).	See under EU	See under EU	Tietosuojavaltuutetun toimisto
France*	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Law No. 78-17 of January 6, 1978 relating to information technology, files and freedoms) (Government of France, 1978[243])	**15**	France is subject to the provisions of the GDPR. Pursuant to GDPR article 8, French law specifies a minimum age of consent as follows: "a minor may consent alone to the processing of personal data concerning the direct offer of information society services from the age of fifteen. Where the minor is under the age of fifteen, processing is lawful only if consent is given jointly by the minor concerned and the holder(s) of parental authority over that minor" (art. 45). The Act further provides that "the data controller shall draft in clear and simple terms, easily understandable by the minor, the information and communications relating to the processing which concerns him".	The CNIL has published guidance on verifying age for the purpose of meeting the requirements of the GDPR, both to confirm if parental consent is required and to trigger special protection for children's data (CNIL, 2021[244]). This guidance specifies that any age assurance solutions must be "analysed in light of the available technologies, taking into account the nature of the proposed processing as well as the associated risks". The guidance further notes, that age assurance solutions should be: • be proportional to risk; • minimise data collection;	See under EU, however France requires joint consent from the child and the parent. The CNIL has published guidance on obtaining parental consent while upholding the child's and parent's privacy (CNIL, 2021[244]). This guidance notes that parental consent mechanisms should: • be proportional to risk; • minimise data collection; • be robust; • be simple and easy to use; and • comply with any industry standards. The guidance further states that third-party solutions that comply with these requirements could be considered.	Commission Nationale de l'Informatique et des Libertés (CNIL)

© OECD 2025

Country / Region	Law	Age Limit	Basis for age limit	Age Assurance Requirement	Requirement for parental consent	Administrator
			The CNIL has published guidance on specific safeguards for protecting the interests of children relevant to their privacy and data protection (CNIL, 2021[244]). The guidance recommends: • deactivating, by default, profiling of minors; and • not reusing or transmitting to third parties children's data for commercial or advertising purposes (unless it can be demonstrate that this is for compelling reasons relating to the best interests of the child).	• be robust; • be simple and easy to use; and • comply with any industry standards. The guidance further states that third-party solutions that comply with these requirements could be considered.		
Germany*	Bundesdatenschutzgesetz (BDSG) (Federal Data Protection Act) (Government of Germany, 2018[245])	**16**	Germany is subject to the provisions of the GDPR and has not made any extra provisions relevant to the age of consent for processing of children's data.	See under EU	See under EU	Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDi)
Greece*	Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data (Government of Greece, 2019[246])	**15**	Greece is subject to the provisions of the GDPR. Pursuant to GDPR article 8, Greek law specifies a minimum age of consent as follows: "1) where [the GDPR] applies, in relation to the offering of information society services directly to a minor, the processing of the personal data of a minor shall be lawful where the minor is at least 15 years old and gives his or her consent; 2) Where the minor is below the age of 15 years, the processing referred to [in 1] shall be lawful only if consent is given by the legal representative of the minor" (at art 21).	See under EU	See under EU	Hellenic Data Protection Authority
Hungary*	Act CXII of 2011 on the right to informational self-determination and on the freedom of information	**16**	Hungary is subject to the provisions of the GDPR and has not made any extra provisions relevant to the age of consent for processing of children's data.	See under EU	See under EU	Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)

© OECD 2025

Country / Region	Law	Age Limit	Basis for age limit	Age Assurance Requirement	Requirement for parental consent	Administrator
	(Government of Hungary, 2024[247])					
Iceland*	Lög um persónuvernd og meðferð persónuupplýsinga (Act on personal protection and processing of personal information) (Government of Iceland, 2018[248])	**13**	Iceland is subject to the provisions of the GDPR. Pursuant to GDPR article 8, Icelandic law specifies a minimum age of consent as follows: "When a child is offered a service in the information society directly and the processing of personal information is based on his consent, the processing is therefore only considered lawful if the child has reached the age of 13. If the child is under 13 years of age, the processing is only considered lawful to the extent that the child's guardian allows consent" (at art 10).	See under EU	See under EU, however the Icelandic law further specifies that "the responsible party shall do what can be considered reasonable to verify (…) that the consent is given or authorized by the guardian of the child, taking into account the available technology." (at art 10).	Persónuvernd vernd
Ireland*	Data Protection Act (Government of Ireland, 2018[249])	**16**	Ireland is subject to the provisions of the GDPR. Pursuant to GDPR article 8, and for these purposes Irish law specifies a minimum age of consent as **16** (at s31). Irish law further specifies that for general purposes (and in accordance with Recital 38 of the GDPR) individuals under the **age of 18** are to be considered children (at s29) and explicitly prohibits direct marketing, profiling or micro-targeting at children as so defined (at s30). Ireland's DPC has published detailed principles and guidance for meeting children's data protection needs (the fundamentals) (Ireland Data Protection Commission, 2021[250]). The fundamentals set out, *inter alia*, that "online service providers should provide a floor of protection for all users, unless they take a risk-based approach to verifying the age of their users" and consequently implement the relevant protections for the processing	The fundamentals set out that age verification is necessary for two reasons: i) to determine if a user is under the **age of 16**, and to consequently know to seek parental consent to process data on the basis of consent; and ii) to determine whether a user is under the **age of 18** and consequently put in place the relevant protections necessary for processing and handling children's data. The fundamentals do not specify specific methods for assuring age, and note that organisations may need to employ a combination of methods, and that the "methods that are most appropriate for organisations will vary considerably from context to context, however, whatever the combination of methods deployed, the result must be demonstrably robust and effective and achieve a level of reliability that is	The fundamentals provide guidance on how the requirement in the GDPR to use "reasonable efforts" to obtain verified consent can be complied with. The fundamentals note that "organisations must fully explore all of the technical options available to them – and maximise innovation". The fundamentals further note that the "methods employed to verify that consent has been obtained from the actual holder of parental responsibility are not overly intrusive and that they adhere to the principles of data protection". They also state that organisations should take a "proportionate approach". The fundamentals give examples of some methods for obtaining verified parental consent (e.g. confirmation email for low risk processing, or payment of a token sum for high risk processing), but the guidance does not prescribe any particular methods for verifying consent.	Data Protection Commission (DPC)

© OECD 2025

Country / Region	Law	Age Limit	Basis for age limit	Age Assurance Requirement	Requirement for parental consent	Administrator
			children's data. The guidance further notes that "online service providers should not profile children and/ or carry out automated decision making in relation to children, or otherwise use their personal data, for marketing/ advertising purposes due to their particular vulnerability and susceptibility to behavioural advertising, unless they can clearly demonstrate how and why it is in the best interests of the child to do so".	commensurate with the risks posed by the processing in question".		
Israel	Protection of Privacy Law (no. 5741-1981) (Government of Israel, 1981[251])	**Not stated**	Israel's privacy law does not set out specific provisions for the protection of children's data. Consent is required for the processing of data (at art. 8), with no specific provisions regarding parental consent. Age of consent, however, is set by Israel's Legal Capacity and Guardianship Law at 18 (Government of Israel, 1962[252]).	N/a	N/a	Ministry of Justice
Italy*	Codice in materia di protezione dei dati personali (Personal Data Protection Code) (Government of Italy, 2003[253])	**14**	Italy is subject to the provisions of the GDPR. Pursuant to GDPR article 8, Italian law specifies a minimum age of consent to data processing at age 14. Below the age of 14, processing the child's data will only be lawful with the consent of the person with parental responsibility. For minors (between 14 & 18), data controllers must use "particularly clear and simple, concise and comprehensive language, easily accessible and understandable by the minor" when obtaining consent in order to make it meaningful (at art. 2-quinquies).	See under EU	See under EU	Garante per la protezione dei dati personali

© OECD 2025

Country / Region	Law	Age Limit	Basis for age limit	Age Assurance Requirement	Requirement for parental consent	Administrator
Japan	Act on the Protection of Personal Information (Act No. 57 of 2003) (Government of Japan, 2003[254])	**Not stated**	Japan's Act (the APPI) itself does not set out specific provisions for the protection of children's data. Consent is required for certain kinds of processing of data (at arts. 18-(1), 20(2), 27(1), 28(1) and 31(1)), with no specific provisions regarding parental consent in the language of the Act. However, Guidelines for the APPI (General Rules Part) clarify that consent should be obtained from a person with parental authority or legal guardian of a minor under the situation where the minor does not have the capacity to judge the consequences of their consent to the processing of data (Personal Information Protection Commission, 2020[255]). The Q&As complementing the Guidelines further clarify that those below age 13 in minimum and those below age 16, depending on situations, fall into the category of a minor lacking capacity to judge the consequences of his/her consent (Personal Information Protection Commission, 2020[256]). In addition, the APPI, together with its delegate act (Cabinet Order) (Government of Japan, 2025[257]), prescribes that certain request relevant to children's data under Article 32(2) to Article 40 of the APPI and Article 76(1) of the APPI) may be made by a legal representative of a minor (Article 13, Item 1 of the Cabinet Order and Article 76(2) of the APPI).	N/a	Parental consent is required when a minor does not have the capacity to judge the consequences of their consent.	Personal Information Protection Commission (PPC)
Korea	Personal Information Protection Act (Government of Korea,	**14**	Korea's Act provides that where consent is required to process personal data, for children under 14 years of age, consent is	While not explicitly dealt with in the Act, standards published by the PIPC, "Online Personal Information	While not explicitly dealt with in the Act, standards published by the PIPC, "Online Personal Information Protection	Personal Information Protection Commission (PIPC)

© OECD 2025

Country / Region	Law	Age Limit	Basis for age limit	Age Assurance Requirement	Requirement for parental consent	Administrator
	2023[258])		to be obtained from the child's legal representative (at art. 22; see also art. 39). The law further states that when notifying children under the age of 14 on issues relevant to the processing of personal information, the data processor must use an easy-to-understand format and clear, easy-to-understand language (at art. 22). Standards published by the PIPC, "Online Personal Information Protection for Children and Adolescents, Principles and Standards" (Korea Personal Information Protection Commission, 2022[259]) set out guidance relevant to targeted advertisements, and note that if online service providers intend to combine children and adolescents' behavioral data with their unique identification information for this purpose they must obtain consent. Even with consent, the guidance recommends that online services should minimise targeted advertising, and not collect or use behavioural data for this purpose for users under 14.	Protection for Children and Adolescents, Principles and Standards" (Korea Personal Information Protection Commission, 2022[259]), sets out guidance relevant to ensuring age. The guidance specifies that if a service is likely to be used by children or adolescents the service should collect information on age in order to verify whether or not the user is under the age of 14 before providing the service. The guidance specifies that for services requiring a registered account, age can be assured by: i) having the user enter their statutory date of birth; or ii) to check a box confirming they are over the age of 14. Noting, that there is a possibility for false age information to be given, the guidance notes that services should require additional age verification processes if a user attempts to change their date of birth from the same IP address, or provide methods for users to report other underage users. In assuring age, the guidance notes that the minimum amount of personal data necessary should be collected.	for Children and Adolescents, Principles and Standards" (Korea Personal Information Protection Commission, 2022[259]), sets out guidance relevant to verifying consent from a parent or legal guardian. Specified methods for such consent are: • authentication via mobile phone, i-PIN, credit card, or joint authentication certificate; • email confirmation; or • indicating consent directly on a webpage, which is then confirmed via SMS.	
Latvia*	Fizisko personu datu apstrādes likums (Personal Data Processing Law)	**13**	Latvia is subject to the provisions of the GDPR. Pursuant to GDPR article 8, Latvian law specifies a minimum age of consent is 13, and that for a child who has not yet reached 13, consent must be	See under EU	See under EU	Datu valsts inspekcija

© OECD 2025

Country / Region	Law	Age Limit	Basis for age limit	Age Assurance Requirement	Requirement for parental consent	Administrator
	(Government of Latvia, 2018[260])		obtained by the child's parent or legal guardian (at art. 33).			
Lithuania*	Lietuvos respublikos Asmens duomenų teisinės apsaugos Įstatymas (Law on Legal Protection of Personal Data) (Government of Lithuania, 1996[261])	**14**	Lithuania is subject to the provisions of the GDPR. Pursuant to GDPR article 8, Lithuanian law specifies that "when information society services are offered directly to a child, the processing of the child's personal data is legal if consent is given by a child at least 14 years old" (at art 6).	See under EU	See under EU	Valstybinė duomenų apsaugos inspekcija
Luxembourg *	Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données (Data Protection Law) (Government of Luxembourg, 2018[262])	**16**	Luxembourg is subject to the provisions of the GDPR and has not made any extra provisions relevant to the age of consent for processing of children's data.	See under EU	See under EU	Commission nationale pour la protection des données (CNPD)
Mexico	Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Federal Law on the Protection of Personal Data Held by Private Parties) (Government of Mexico, 2010[263])	**18**	Mexico's privacy law does not set out specific provisions for the protection of children's data. Consent is required for the processing of data (at art. 8), with no specific provisions regarding parental consent. Nonetheless, as a product of Mexico's constitution (which recognises children as rights holders and defines them as persons under 18), children have a constitutional right to the protection of their data (Government of Mexico, 1928[264]). Children are assumed not to have capacity for valid consent to the processing of that data, and as such parental consent is required (Government of Mexico,	N/a	N/a	(Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales) (INAI)

© OECD 2025

Country / Region	Law	Age Limit	Basis for age limit	Age Assurance Requirement	Requirement for parental consent	Administrator
			2024[265]). Mexico's privacy enforcement authority has published a code of good practice relevant to processing children's data (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, 2020[266]).			
Netherlands *	Uitvoeringswet Algemene verordening gegevensbescherming (General Data Protection Regulation Implementation Act) (Government of the Netherlands, 2018[267])	**16**	The Netherlands is subject to the provisions of the GDPR. Pursuant to GDPR article 8, the Netherlands law (at art 5) specifies: • "Where Article 8 of the Regulation does not apply, the consent of the data subject shall be replaced by that of his or her legal representative if the data subject has not yet reached the age of sixteen; • "Consent may be withdrawn at any time by the data subject's legal representative". • [GDPR data subject rights] may be exercised by the legal representatives of persons under the age of 16.	The Netherlands law does not specify any requirement for age assurance, however the Netherlands Code for Children's Rights (code voor kinderrecthten) (Government of the Netherlands, 2021[268]) provides guidance on assuring age for the purpose of complying with privacy law. The Code specifies that for privacy age assurances is necessary to i) determine if a user is under the **age of 16**, and to consequently know to seek parental consent to process data on the basis of consent; and ii) determine whether a user is under the **age of 18** and consequently put in place the relevant protections necessary for processing and handling children's data. Specific examples of age assurance methods that are given include: • self-declaration (in low risk cases) • technical measures; • use of a third-party age assurance service; • confirmation of age by the	Beyond the requirement in the GDPR, the Netherlands law does not specify how parental consent may be obtained/verified. The Netherlands Code for Children's Rights (code voor kinderrecthten) (Government of the Netherlands, 2021[268]) notes that "reasonable efforts must be made to verify (parental consent) through means that satisfy the state of the art. When building in age verification and verification of parental consent, no more personal data may be processed than is strictly necessary".	Autoriteit Persoonsgegevens

© OECD 2025

Country / Region	Law	Age Limit	Basis for age limit	Age Assurance Requirement	Requirement for parental consent	Administrator
				parent via text or email. In assuring age, the guidance specifies that services should only process the minimum amount of data necessary to assure age.		
New Zealand	Privacy Act (2020) (Government of New Zealand, 2020[269])	**No set age**	In general, New Zealand's Privacy Act provides children with the same privacy protections and rights as adults. However, the law does note that when collecting data from a child or young person, any agency collecting the data must do so in a manner that is "fair", and "does not intrude to an unreasonable extent upon the personal affairs of the individual concerned" (at s22, Information Privacy Principle 4). The law does not define "child or young person".	N/a	The law does not set out a requirement for verified parental consent. Guidance from New Zealand's privacy Commissioner does note that for "very young children who simply aren't able to act on their own behalf" agencies should "take a practical approach and consider whether the child's parent/s or guardian/s are acting as the child's representative" (New Zealand Privacy Commissioner, 2013[270]).	Privacy Commissioner
Norway*	Personopplysningsloven (Act on the Processing of Personal Data) (Government of Norway, 2018[271])	**13**	Norway is subject to the provisions of the GDPR, and for the purposes of GDPR article 8, Norwegian law sets the age limit for consent at 13 (§ 5).	See under EU	See under EU	Datatilsynet
Poland*	Ustawa o ochronie danych osobowych (Act on the Protection of Personal Data) (Government of Poland, 2018[272])	**16**	Poland is subject to the provisions of the GDPR and has not made any extra provisions relevant to the age of consent for processing of children's data.	See under EU	See under EU	Urząd Ochrony Danych Osobowyc (UODO)
Portugal*	Lei de Proteção de Dados Pessoais (Personal Data Protection Law)	**13**	Portugal is subject to the provisions of the GDPR, and for the purposes of GDPR article 8, Portuguese law sets the age limit for consent at 13, and provides that, "if the child is under the age of 13, the processing	See under EU	See under EU, though Portuguese law does additionally refer to "secure authentication means". The law does not specify what these means could be.	Comissão Nacional de Proteção de Dados (CNPD)

© OECD 2025

Country / Region	Law	Age Limit	Basis for age limit	Age Assurance Requirement	Requirement for parental consent	Administrator
	(Government of Portugal, 2019[273])		shall only be lawful if consent is given by the child's legal representatives, preferably using secure authentication means" (at art 16).			
Slovak Republic*	Zakon z 29. novembra 2017 o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (Law on the Protection of Personal Data) (Government of the Slovak Republic, 2018[274])	**16**	The Slovak Republic is subject to the provisions of the GDPR, and for the purposes of GDPR article 8, Slovak Republic law sets the age limit for consent at 16, specifying that, "if the person concerned is under 16 years of age, such processing of personal data is legal only under the conditions and to the extent that such consent has been given or approved by their legal representative" (at § 15).	See under EU	See under EU, though Slovak Republic law additionally specifies that, "The operator is obliged to make reasonable efforts to verify that the legal representative of the person concerned has given or approved consent to the processing of personal data (…) taking into account the available technology" (at § 15).	Úrad na ochranu osobných údajov (UOOU)
Slovenia*	Zakon o varstvu osebnih podatkov (ZVOP-2) (Personal Data Protection Act) (Government of Slovenia, 2022[275])	**15**	Slovenia is subject to the provisions of the GDPR, and for the purposes of GDPR article 8, Slovenian law sets the age limit for consent at 15, specifying that: "if the child is under 15 years of age, consent is only valid if it is given or approved by one of the child's parents, his guardian or a person to whom parental care is granted" (at art 8). The law further notes that the child's consent "must not be conditioned by excessive conditions on the part of the controller" and require more personal data than necessary for the specific purpose (at art 8).	See under EU	See under EU	Informacijski pooblaščenec
Spain*	Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (Organic Law on Data Protection and the Guarantee of Digital	**14**	Spain is subject to the provisions of the GDPR, and for the purposes of GDPR article 8, Spanish law sets the age of consent at 14, expressly noting that the "processing of data of minors under fourteen years of age, based on consent, will only be lawful if the consent of the holder of parental authority or guardianship	See under EU	See under EU	Agence espagnole de protection des données (AEPD)

© OECD 2025

Country / Region	Law	Age Limit	Basis for age limit	Age Assurance Requirement	Requirement for parental consent	Administrator
	Rights) (Government of Spain, 2018[276])		is provided" (art. 7).			
Sweden*	Dataskyddslagen (Data Protection Act) (Government of Sweden, 2018[277])	**13**	Sweden is subject to the provisions of the GDPR. Pursuant to GDPR article 8, Swedish law (at § 2, 4) specifies that: • Information society services that offer services directly to a child living in Sweden who is 13 or older, can only process that child's personal data with the child's consent; and • For children under 13 years of age, such data processing is only permitted if consent is given or approved by the person who has parental responsibility for the child".	See under EU	See under EU	Integritetsskyddsmyndigheten (IMY)
Switzerland	Federal Act on Data Protection (FAPD) (2020) (Government of Switzerland, 2020[278])	**Not stated**	Swiss law provides neither specific protections for processing children's data, nor specific provisions regarding children's capacity to consent to the processing of data. Consent to process data is required only in certain circumstances (processing sensitive personal data; high-risk profiling by a private person; or profiling by a federal body) (see art. 6(7)) and in these cases consent must be explicit, In certain circumstances, Swiss law allows the processing of data without consent (arts. 30,31,34). The Swiss Civil Code provides that persons under the age of 18 lack capacity (see arts. 13-19) (Government of Switzerland, 1907[279]). Should a child under 18 need to consent, it is therefore	N/a	N/a	Federal Data Protection and Information Commissioner (FDPIC)

© OECD 2025

Country / Region	Law	Age Limit	Basis for age limit	Age Assurance Requirement	Requirement for parental consent	Administrator
			likely that they would need a representative to act on their behalf.			
Türkiye	KVKK - Kişisel Verilerin Korunması Kanunu (Law on the Protection of Personal Data) (Government of Türkiye, 2016[280])	**No set age**	Türkiye's privacy law does not set out specific provisions for the protection of children's data. Consent is required for the processing of data, including in circumstances where a person's consent is not legally valid (at art. 5). The law does not specify if this refers to children, however according to the Civil Code the national age of majority is 18 (at art. 11) (Government of Türkiye, 2001[281]). However, guidance from the KVKK does note that when processing children's data, data controllers should adopt the highest level of technical and administrative measures to ensure data security when processing children's data (KVKK, 2020[282]).	The law does not set out a requirement for age assurance. However, guidance from the KVKK directed at the developers of digital products and services notes that, considering current available technology, systems should be used to verify a child's age (KVKK, 2020[282]).	The law does not set out a requirement for verified parental consent. However, guidance from the KVKK does note that when needed, information about the data processing and explicit requests for consent can be sent to a verified parent or guardian (KVKK, 2020[282]).	Kisisel Verileri Koruma Kurumu (KVKK)
United Kingdom	Data Protection Act (2018) (Government of the United Kingdom, 2018[283]) UK GDPR (2016) (Government of the United Kingdom, 2020[284]) ICO's age-appropriate design code (United Kingdom Information Commissioners Office, 2020[77])	**18**	UK's privacy law reflects the GDPR, and children are subject to the same data protection rights as adults. The main rules regarding children's data are contained within the Children's Code, a regulatory code established pursuant to the Data Protection Act (at s123). Children are able to exercise their data rights if they are competent to do so. In Scotland, a person aged 12 or over is "presumed to be of sufficient age and maturity to be able to exercise their data protection rights, unless the contrary is shown". In England, Wales and Northern Ireland competence is assessed "depending upon the level of understanding of the child". A child that is	Information society service's likely to be accessed by children, are required to put in place an "age-appropriate application" of the provisions of the Children's Code. The ICO's age-appropriate design code (at part 3) sets out that to do this, services will need to establish "with a level of certainty that is appropriate to the risks to the rights and freedoms that arise from (their) data processing what age range (their) individual users fall into". If age is not established, then the service is required to "apply all standards of the code to all users in a risk-based and proportionate way". The code further notes that if a service	The Children's Code (at Annex C) notes that parental consent for users under **13** will need be obtained when: a) a service is made available to children; and b) consent is being relied on as the lawful basis for processing. The ICO's age-appropriate design code specifies that (in accordance with the UK GDPR) states that "reasonable efforts" should be made to obtain and verify parental consent for children under 13. It further states that the data processor can "take available technology into account in deciding what is reasonable", and that other circumstances can also be considered, including resources and the level of risk identified in a data	Information Commissioner's Office (ICO)

© OECD 2025

Country / Region	Law	Age Limit	Basis for age limit	Age Assurance Requirement	Requirement for parental consent	Administrator
			clearly acting against their own best interests should not be considered competent (United Kingdom Information Commissioners Office, 2025[285]). When data is processed by an information society service on the lawful basis of consent (as per the GDPR), the relevant age for a child to be able to give consent is **13,** for children under that age parental consent must be given (see ICO's age-appropriate design code at Annex C). The ICO's age-appropriate design code requires an age-appropriate application of services that are used or likely to be used by children. The ICO's age-appropriate design code further notes that the use of a child's data to profile them for the purposes of targeted advertising must be off by default, unless it can be shown to be in the best interest of the child.	is an adult directed one in any event, service providers should focus on ways to prevent access rather than on ways to accommodate child users. The ICO has published guidance on age assurance (United Kingdom Information Commissioners Office, 2024[286]). While the guidance gives examples of different types of age assurance, it does not prescribe specific methods. It does recommend that age assurance approaches should: i) be informed by the services risk profile; ii) have an appropriate level of technical accuracy, reliability and robustness; and iii) be operated in a "fair way". The guidance further states that information society services should check whether the age assurance solution is certified against recognised industry standards. The ICO guidance further notes that in implementing age assurance, consideration must be given to: i) the least privacy intrusive approach; and ii) obligations under other laws (i.e. the Online Safety Act).	protection impact assessment, but that the approach must be able to be justified.	
United States	Children's Online Privacy Protection Act (COPPA) (Government of the United States, 1998[287])	**13**	COPPA defines a child as any person under the age of 13 and requires that websites and online services: • obtain parental (including legal guardian) consent for processing a child's data under that age; and • put in place specific protections when processing the data of children	N/a	The COPPA rule states that "obtaining verified parental consent means making any reasonable effort (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child: (1) Receives notice of the operator's personal information	Federal Trade Commission (FTC)

© OECD 2025

Country / Region	Law	Age Limit	Basis for age limit	Age Assurance Requirement	Requirement for parental consent	Administrator
			under the age of 13. Where a website or online service is either directed at a child or has actual knowledge that a child is accessing their service, and that service fails to meet the above requirements, they are in violation of COPPA and will face penalties. The COPPA Rule (United States Code of Federal Regulations, 2013[19]) establishes the specific protections for processing children's data and requires that websites and online services: • establish and maintain reasonable procedures to protect the confidentiality, security and integrity of children's personal information; • provide notice on what information it collects from children, how it uses such information, and its disclosure practices for such information; • provide reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance; and • do not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity. The COPPA Rule further provides that any data collected for supporting a website or		collection, use, and disclosure practices; and (2) Authorizes any collection, use, and/or disclosure of the personal information". The COPPA Rule further notes that "any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent", and that existing methods that meet this requirement include: • providing a consent form that can be signed by the parent and returned by mail, facsimile, or electronic scan; • having a parent, in connection with a financial transaction, use a credit card, debit card or other online payment system that provides a notification of each transaction to the primary account holder; • having a parent call a toll-free telephone number staffed by trained personnel; • having a parent connect to trained personnel via video-conference; • checking a form of the parent's government-issued identification against a relevant database (and deleting that identification promptly after conducting the check); and • provided that no personal information of the child is disclosed, using an email coupled with additional steps (e.g.	

© OECD 2025

Country / Region	Law	Age Limit	Basis for age limit	Age Assurance Requirement	Requirement for parental consent	Administrator
			online services internal operations, cannot be used to "contact a specific individual, including through behavioral advertising, to amass a profile on a specific individual, or for any other purpose".		confirmatory email, mail, or phone call) to ensure that the person providing consent is in fact the parent.	

"*" Denotes EU/EEA Member States that are subject to the provisions of the GDPR

© OECD 2025

Annex E. Laws regulating online purchase of physical products

The tables in this annex set out age limits relevant to the online purchase of age-restricted physical goods, covering alcohol (Table A E.1), cigarettes (Table A E.2), and knives (Table A E.3).

Where a law expressly prohibits the sale of the item online, or expressly requires that a physical ID be sighted on delivery, the column setting out any "online age assurance" requirement is marked "N/a", given that a prohibition on children having these "adult goods" delivered directly to them is already covered in the law. When the entry in this column is "unclear", it indicates that a country's law prohibits the sale of such goods to children but does not address online sales, or a need to see an ID, or both.

In jurisdictions where the applicable laws are decentralised, the legal frameworks for the sale of these goods are often dealt with at the state or provincial level. This means that there could be several laws in each country covering the field. Given the volume of laws that would be required to be reviewed to cover each decentralised jurisdiction, the tables include only OECD Member countries with a centralised legal approach. However, with regard to those OECD Member countries whose laws have not been mapped, where there is relevant research or evidence concerning the sale and delivery of such goods in their country that is relevant to online age assurance, they may nonetheless be considered in the main body of the report.

Table A E.1. Age limits and age assurance requirements in laws regulating sale of alcohol

Country / Region	Law	Age Limit	Can the good be delivered without a physical ID check?	If yes, what (if any) is the online age assurance requirement?	Administrator
Australia	Laws differ across states.				
Austria	Laws differ across states.				
Belgium	Loi relative à la protection de la santé des consommateurs en ce qui concerne les denrées alimentaires et les autres produits	**16** (beers & wines) **18** (alcohol > 0.5% volume)	Unclear. The law does not provide specific provisions regarding the sale of alcohol products.	Unclear	Federal Public Service for Public Health, Food Chain Safety and the Environment

© OECD 2025

Country / Region	Law	Age Limit	Can the good be delivered without a physical ID check?	If yes, what (if any) is the online age assurance requirement?	Administrator
	(Law on the Protection of the Health of Consumers with regard to Foodstuffs and Other Products) (Government of Belgium, 1997[288])				
Canada	Laws differ across provinces				
Chile	Ley Sobre Expendio Y Consumo De Bebidas Alcoholicas (Law on The Sale And Consumption Of Alcoholic Beverages) (Government of Chile, 2024[289])	**18**	Unclear. The sale of alcohol without sighting identification documents is prohibited (at art. 42). It is unclear if this extends to a need to sight identity on delivery.	Unclear	Ministry of Health
Colombia	Ley 124 De 1994 por la cual se prohíbe el expendio de bebidas embriagantes a menores de edad y se dictan otras disposiciones (Law by which the sale of intoxicating beverages to minors is prohibited and other provisions are issued) (Government of Colombia, 1994[290])	**18**	Unclear. The law prohibits the sale of alcohol to minors (at art. 1), and a Decree giving effect to the law calls for ID checks when there is doubt as to a customer's age (at art. 12) (Government of Colombia, 2010[291]). It is unclear if this extends to a need to sight identity on delivery.	Unclear	Ministry of Health
Costa Rica	Regulación De Horarios De Funcionamiento En Expendios De Bebidas Alcohólicas (Regulation of Operating Hours in Alcoholic Beverage Outlets) (Government of Costa Rica, 1996[292])	**18**	Unclear. The law prohibits the sale of alcohol to minors (at art. 1), however it does not deal with a need to assure age, or with online sales/deliveries. **Minor** is not defined in this law however Costa Rica's Civil Code defines them as individuals who have not yet reached 18 (at	Unclear	Municipalities

© OECD 2025

Country / Region	Law	Age Limit	Can the good be delivered without a physical ID check?	If yes, what (if any) is the online age assurance requirement?	Administrator
			art 37) (Government of Costa Rica, 1985[180]).		
Czechia	Zákon č. 65/2017 Sb. Zákon o ochraně zdraví před škodlivými účinky návykových látek (Act on the Protection of Health from the Harmful Effects of Addictive Substances) (Government of Czechia, 2017[293])	**18**	No. A person who sells alcoholic beverages via distance communication is obliged to collect the name, address, and identification number of the person at the point of delivery. (at § 15)	N/A	Ministry of Health.
Denmark	Herved bekendtgøres lov om forbud mod salg af tobak og alkohol til personer under 18 år (Executive Order on the Prohibition of the Sale of Tobacco and Alcohol to Persons Under the Age of 18) (Government of Denmark, 2008[294])	**16** (alcohol <16.5%) **18** (alcohol > 16.5%)	Unclear Vendors are required to ask for ID to verify age at the point of sale (at § 2), however the law does not deal with online sales.	Unclear	The Minister for Health and Prevention
Estonia	Alkoholiseadus (Alcohol Act) (Government of Estonia, 2002[295])	**18**	No. The sale of alcohol to minors is prohibited, and the seller is required to sight ID at both the point of sale, and the point of delivery (at § 47). Minor is not defined in the Act, but Estonia's child protection law establishes that a child is every person under 18 (at §3(2)) (Government of Estonia, 2014[183]).	N/a	Supervisory authorities set out by Chapter 4, § 49.
Finland	Alkoholilaki (Alcohol Act)	**18**	Unclear.	Unclear	The Ministry of Social Affairs and Health

© OECD 2025

Country / Region	Law	Age Limit	Can the good be delivered without a physical ID check?	If yes, what (if any) is the online age assurance requirement?	Administrator
	(Government of Finland, 2017[296])		The law prohibits the sale of alcohol to children (at s37(1)) and requires proof of age at point of sale (at s40). However, the law does not deal with online sales. A 2024 Bill would amend the alcohol act to provide for *inter alia* age assurance (including via electronic means) for the delivery of alcoholic beverages. However, as of March 2025 it is not yet enacted. (Government of Finland, 2024[297])		
France	Code de la santé publique (Health Code) (Government of France, 1953[298])	**18**	Unclear. The sale of alcohol to minors is prohibited, and any person who hands over the alcohol is required to ask the customer for proof of ID (art. L3342-1) however the law does not deal with online sales. Minor is not defined, but is defined as persons under 18 in the French Civil Code (Government of France, 1804[109])	Unclear	Direction générale de la Santé (DGS)
Germany	Jugendschutzgesetz (JuSchG) (Youth Protection Act) (Government of Germany, 2002[112])	**16** (Beer & wine) **18** (Other alcohols)	Unclear. The law prohibits the sale of alcohol to minors under 16 (for beer and wine) or to all minors (fpr other alcohols;at § 9), and implicitly provides for an obligation to verify age in mail order purchases (§ 2 (2)).	Unclear	Local regulatory authorities
Greece	Protection of minors from tobacco and alcoholic beverages and other provisions (Government of Greece, 2008[299])	**18**	Unclear. The sale of alcohol to minors is prohibited (at art 4), however the law does not deal with online sales, or specify a requirement to sight ID.	Unclear	Ministry of Health and Social Solidarity

© OECD 2025

Country / Region	Law	Age Limit	Can the good be delivered without a physical ID check?	If yes, what (if any) is the online age assurance requirement?	Administrator
Hungary	1997. évi CLV. Törvény a fogyasztóvédelemről (Act on consumer protection) (Government of Hungary, 1997[300])	**18**	Unclear. The sale of alcohol to minors is prohibited (at §16/A(1)), and proof of age is required at point of sale (at §16/A(4)). However, the law does not deal with online sales.	Unclear	Hungarian Competition Authority
Iceland	Áfengislög (Alcohol Act, 1998) (Government of Iceland, 1998[301])	**20**	No. The law prohibits the sale, provision or **delivery** of alcohol to anyone under the age of 20 years. If the person delivering the alcohol has a reason to believe that the recipient is not yet 20 years of age, then the deliverer must check the recipients ID (at art. 18).	N/a	Ministry of Justice
Ireland	Intoxicating Liquor Act (Government of Ireland, 1988[302])	**18**	No. The law prohibits the sale or **delivery** of alcohol to anyone under the age of 18 years (at s31(1)(2)), and states that verifying ID at point of sale or delivery is a defense to contravening this prohibition (at s 31(4)). The law does however permit the delivery of alcohol to persons under 18 at a private residence (at s31(2)).	N/a	Minister for Justice, Equality and Law Reform
Israel	Penal Code (Government of Israel, 1977[185])	**18**	Unclear. The sale of alcohol to minors is prohibited and requires ID checks for this purpose (at art 193). However the law does not deal with online sales.	Unclear	Minister of the Interior
Italy	Legge quadro in materia di alcol e di problemi alcolcorrelati (Framework law on alcohol and alcohol-related problems.)	**18**	Unclear. The law prohibits the sale of alcohol to persons under 18 and requires ID checks for this purpose (at art. 14ter). The law does	Unclear	Minister of Health

© OECD 2025

Country / Region	Law	Age Limit	Can the good be delivered without a physical ID check?	If yes, what (if any) is the online age assurance requirement?	Administrator
	(Government of Italy, 2001[303])		not deal with online sales.		
Japan	Law concerning the prohibition of drinking by persons under the age of 20 (Government of Japan, 1922[304])	**20**	No. The law prohibits the sale of alcohol to persons under 20 and requires sellers to verify the purchaser's age (Article 1.4). The law does not cover online sales, but proof of purchaser's age is required for online sales.	N/A	National Police Agency
Korea	Youth Protection Act (Government of Korea, 1997[128])	**19**	No. "The law defines alcohol as a drug harmful to youth (at art. 2(4)), and prohibits the sale of alcohol to minors, including via communication devices (at art. 28(1)). It requires a seller to verify the age of any purchaser (at art. 28(4)), and this is done through age verification methods. Korea prohibits online alcohol sales, except for traditional alcohol (at the Notification on the Electronic Transaction of Alcoholic Beverages), and the sale of alcohol via communication devices is possible only after the purchaser is verified to be of adult age through age verification methods.	The online age assurance requirement is contained in the Notification on the Electronic Transaction of Alcoholic Beverages (Government of Korea, 2025[305])(at art. 5, para 1). Acceptable age assurance measures are: • Digital certificate under the Digital ASignature Act • Internet personal identification number (I-PIN), • Age verification methods provided by electronic signature certification service providers, • Mobile resident registration card, • Mobile driver's license, • Mobile national veterans' registration certificate, • Mobile foreigner registration certificate under the Immigration Control Act."	Ministry of Gender Equality and Family (Youth Protection and Environment Division)
Latvia	Alkoholisko dzērienu aprites likums (Handling of Alcoholic Beverages Law) (Government of Latvia, 2004[306])	**18**	Yes. The law prohibits the sale of alcohol to persons under 18 and requires ID checks for this purpose (at s 6). The law expressly allows for the sale of alcohol online, requiring ID on point of delivery when a "natural person"	For the purpose of the law, "electronic means" refers to using: • qualified means of electronic identification; or • qualified means of electronic identification of increased safety; or • means of electronic identification of a person that conform to the requirements for the safe authentication of users, laid	Ministry of Health

© OECD 2025

Country / Region	Law	Age Limit	Can the good be delivered without a physical ID check?	If yes, what (if any) is the online age assurance requirement?	Administrator
			intermediary conducts the delivery. When there is no intermediary, age verification is to occur via electronic means (at s6[1])	out in the EU Directive on payment services in the Internal Market (European Commission, 2015[307]).	
Lithuania	Alkoholio Kontrolės Įstatymas (Alcohol Control Law) (Government of Lithuania, 1995[308])	**18**	Unclear. The law prohibits the sale of alcohol to persons under 18 (at art. 18(3)(5)). However the law does not refer to a need for ID checks and does not deal with online sales.	Unclear	Drug, Tabaco and Alcohol Control Department (NTAKD)
Luxembourg	Loi du 22 décembre 2006 portant interdiction de la vente de boissons alcooliques à des mineurs de moins de seize ans (Act prohibiting the sale of alcoholic beverages to minors under the age of sixteen) (Government of Luxembourg, 2006[309])	**16**	Unclear. The law prohibits the sale of alcohol to persons under 16. However, the law does not refer to a need for ID checks and does not deal with online sales.	Unclear	Ministry of Health
Mexico	Ley General de Salud (The General Health Law) (Government of Mexico, 1984[310])	**18**	Unclear The law prohibits the sale of alcohol to persons under 18 (at art. 220). However, the law does not refer to a need for ID checks and does not deal with online sales.	N/A	Ministry of Health, the governments of the federal entities, General Health Council.
Netherlands	Alcoholwet (Alcohol Act, 2021) (Government of the Netherlands, 2021[311])	**18**	No. Sellers must both engage in an age verification process at point of sale and confirm identification and age on delivery (at Art. 20a). Methods for undertaking the age verification process are not set out.	N/a	Ministry of Health, Welfare & Sport (National Level) Mayors (Municipal Level)

© OECD 2025

Country / Region	Law	Age Limit	Can the good be delivered without a physical ID check?	If yes, what (if any) is the online age assurance requirement?	Administrator
New Zealand	Sale and Supply of Alcohol Act (2012) (Government of New Zealand, 2012[312])	**18**	Yes. The law permits the sale of alcohol by distance (s18) and does not explicitly address age verification for this purpose.	The law does not prescribe an online age assurance process. The law does not positively require a seller to assure age prior to purchase but does create a defense to supplying alcohol to children if the seller "verified the customer's age using an approved evidence of age system in the approved manner" (s239). Regulations specify "approved" documents, which are all physical ID. They do not specify what is an "approved manner" (Government of New Zealand, 2013[313])	Alcohol Regulatory and Licensing Authority
Norway	Alkoholloven – alkhl (Alcohol Act) (Government of Norway, 1990[314])	**20** (22-60% alcohol volume) **18** (0.7 – 21% alcohol volume)	Unclear The law prohibits the sale of alcohol to persons under 18 (at § 1-5.). However, the law does not refer to a need for ID checks and does not deal with online sales.	Unclear	Ministry of Health and Care Services
Poland	Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (Act Sobriety Education and Counteracting Alcoholism) (Government of Poland, 1982[315])	**18**	Unclear. The law prohibits the sale of alcohol to persons under 18 and requires ID checks for this purpose (at art. 15). However, the law does not deal with online sales.	Unclear	Ministry of Health
Portugal	Decreto-Lei.º 50/2013, de 16 de abril (Decree-Law No. 50/2013) (Government of Portugal, 2013[316])	**16** (beers & wines) **18** (spirits)	Unclear. The law prohibits the sale of alcohol to persons under 18 and requires ID checks for this purpose (at art. 3). However, the law does not deal with online sales.	Unclear	Ministry of Health
Slovak Republic	Zákon č. 219/1996 Z. z. Zákon Národnej rady Slovenskej republiky o ochrane pred zneužívaním	**18**	Unclear. The law prohibits the sale of alcohol to persons under 18 (at §2) and requires ID	Unclear	Ministry of Health

© OECD 2025

Country / Region	Law	Age Limit	Can the good be delivered without a physical ID check?	If yes, what (if any) is the online age assurance requirement?	Administrator
	alkoholických nápojov a o zriaďovaní a prevádzke protialkoholických záchytných izieb (Act of the National Council of the Slovak Republic on Protection against the Abuse of Alcoholic Beverages and on the Establishment and Operation of Anti-Alcohol Detention Rooms) (Government of the Slovak Republic, 1996[317])		checks for this purpose (at §3). However, the law does not deal with online sales.		
Slovenia	Zakona o omejevanju porabe alkohola (Act on the Restriction of Alcohol Consumption) (Government of Slovenia, 2003[318])	**18**	Unclear. The law prohibits the sale of alcohol to persons under 18 (at art. 7) and requires ID checks for this purpose (at art. 8). However, the law does not deal with online sales.	Unclear	Ministry of Health
Spain	Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana (Law on the Protection of Public Safety) (Government of Spain, 1992[319])	**18**	Unclear. The law prohibits the sale of alcohol to minors (at art. 26(d)). However, the law does not refer to a need for ID checks and does not deal with online sales. Minor is not defined in the law, however Spain's Civil Code (Government of Spain, 1889[144]) defines the age of majority as 18 (at art 315).	Unclear	Minister of Interior
Sweden	Alkohollag (Alcohol Act) (Government of Sweden, 2010[320])	**20** (Spirits) **18** (Other alcohols)	Unclear. The law prohibits the sale of alcohol to persons under 20 or 18 (at s 7). However, the law does not refer to a need for ID checks and does not deal with online sales.	Unclear	Ministry of Health and Social Affairs

© OECD 2025

Country / Region	Law	Age Limit	Can the good be delivered without a physical ID check?	If yes, what (if any) is the online age assurance requirement?	Administrator
Switzerland	Alkoholgesetz, AlkG (Federal Law on Spirits) (Government of Switzerland, 1932[321])	**18** (Spirits) **16** (Beer, wine & cider)	Unclear. The law prohibits the delivery of alcohol to children, however it does not specify any mechanisms for assuring age at either point of sale or point of delivery.	Unclear	Alcohol Division (ALK) of the Federal Office for Customs and Border Security FOCBS
Türkiye	İspirto Ve İspirtolu İçkiler İnhisari Kanunu (Spirit Beverages Law) (Government of Türkiye, 1942[322])	**18**	No. It is prohibited to both sell alcohol to children, or via mail order (at art. 6).	N/a	Ministry of Agriculture and Forestry of Türkiye
United Kingdom	Licensing Act (England, Wales, Northern Ireland) (UK Public General Acts, 2003[323]) Licensing (Scotland) Act (Parliament of Scotland, 2005[324]) *Laws have like provisions*	**18**	No. The law prohibits the sale of alcohol to children and requires the seller to take reasonable steps to establish the buyers age. Asking for evidence of age is considered a reasonable step (at s146, E/W/NI; s102 S). It is likewise prohibited to deliver alcohol to a child. The E/W/NI act does not precise a need to sight evidence of age in this section (s151), however the Scottish Act does (s108).	N/a	Authorities differ across jurisdictions.
United States	Laws differ across States				

© OECD 2025

Table A E.2. Age limits and age assurance requirements in laws regulating sale of cigarettes

Country / Region	Law	Age Limit	Can the good be delivered without a physical ID check?	If yes, what (if any) is the online age assurance requirement?	Administrator
Australia	Laws differ across states.				
Austria	Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Tabak- und Nichtraucherinnen- bzw. Nichtraucherschutzgesetz (Tobacco and Non-Smoker Protection Act - Federal Consolidated) (Government of Austria, 2024[325])	**18**	No. The law expressly prohibits both the sale of tobacco products to persons under the age of 18, and their sale by mail order (§ 2a).	N/A	Federal Ministry of Health
Belgium	Loi relative à la protection de la santé des consommateurs en ce qui concerne les denrées alimentaires et les autres produits (Law on the Protection of the Health of Consumers with regard to Foodstuffs and Other Products) (Government of Belgium, 1997[288])	**18**	Unclear. Vendors are required to ask the customer to prove they are above the age of 18 in case they appear to be under the age of 25 (at § 4), however, it is not specified whether this applies to online sales and deliveries as well.	Unclear	Federal Public Service for Public Health, Food Chain Safety and the Environment
Canada	Laws differ across provinces.				
Chile	Ley 19419 Regula Actividades Que Indica Relacionadas Con El Tabaco (Regulates Activities Related to Tobacco) (Government of Chile, 1995[326])	**18**	Unclear Vendors are required to ask for ID to verify age at the point of sale (at art 12), however the law does not deal with online sales.	Unclear	Ministry of Health
Colombia	Ley Número 1335 De 2009 (Provisions to prevent damage to the health of minors) (Government of Colombia, 2009[327])	**18**	Unclear Vendors are required to ask for ID to verify age at the point of sale (at art 2), however the law does not deal with online sales.	Unclear	Ministries of Welfare and National Education
Costa Rica	Ley General De Control Del Tabaco Y Sus Efectos Nocivos En La Salud (General Law On	**18**	No. The law expressly prohibits both the sale of tobacco	N/a	Ministry of Health

© OECD 2025

Country / Region	Law	Age Limit	Can the good be delivered without a physical ID check?	If yes, what (if any) is the online age assurance requirement?	Administrator
	Tobacco Control and Its Harmful Effects on Health) (Government of Costa Rica, 2012[328])		products to persons under the age of 18 (at art. 36.c.vii), and their sale by "telephone, digital, electronic, mail and other means by which the identification of the buyer cannot be clearly and promptly verified" (at art. 16).		
Czechia	Zákon č. 65/2017 Sb. Zákon o ochraně zdraví před škodlivými účinky návykových látek (Act on the Protection of Health from the Harmful Effects of Addictive Substances) (Government of Czechia, 2017[293])	**18**	Yes. The law expressly prohibits the sale of tobacco products to persons under the age of 18 (see § 3(4)), including by distance (see §6 (1)). However, the law establishes a requirement for online age verification for this purpose and only specifies a point of sale ID check, and not at point of delivery.	Sales by distance require the seller to be equipped with a system that electronically verifies the consumers age through a means of remote communication (see §6 (1)). The vendor is required to collect the name, address of the registered office and identification number of the customer when pertaining sale over means of distance communication (see §6 (3)), and is prohibited from using the buyers personal data for any purpose not connected to the sale (see §6 (7)).	Ministry of Health
Denmark	Herved bekendtgøres lov om forbud mod salg af tobak og alkohol til personer under 18 (Executive Order on the Prohibition of the Sale of Tobacco and Alcohol to Persons Under the Age of 18) (Government of Denmark, 2008[294])	**18**	Unclear Vendors are required to ask for ID to verify age at the point of sale (at § 2.a), however the law does not deal with online sales.	Unclear	Minister for Health and Prevention
Estonia	Tubakaseadus (Tobacco Act) (Government of Estonia, 2005[329])	**18**	No. The law expressly prohibits both the sale of tobacco products to persons under the age of 18 (at § 28), and their sale by distance (§ 31).	N/a	Board of Health
Finland	Tobakslag (Tobacco law) (Government of Finland,	**18**	No. The law expressly prohibits both the sale of tobacco products to persons under the age of 18 (at §53), and	N/a	Ministry of Social Affairs and Health

© OECD 2025

Country / Region	Law	Age Limit	Can the good be delivered without a physical ID check?	If yes, what (if any) is the online age assurance requirement?	Administrator
	2016[330])		their sale by distance (§58).		
France	Code de la santé publique (Public Heath Code) (Government of France, 1953[298])	**18**	Unclear. The sale of tobacco products to minors is prohibited (at art L3512-1-1), and any person who hands over tobacco products is required to ask the customer for proof of age (at art. L3512-12) however the law does not deal with online sales.	Unclear	Direction générale de la Santé (DGS)
Germany	Jugendschutzgesetz (JuSchG) (Youth Protection Act) (Government of Germany, 2002[112])	**18**	Unclear The sale of tobacco products to minors is prohibited, and the law expressly provides that such products cannot be offered or sold to children by mail order (at § 10).	The law provides for age assurance requirements (at § 1 (4)), stating that "technical or other precautions" should be taken to prevent the delivery of cigarettes to children.	Local regulatory authorities
Greece	Protection of minors from tobacco and alcoholic beverages and other provisions (Government of Greece, 2008[299])	**18**	Unclear. The sale of tobacco products to minors is prohibited (at art 2(1)(a)), however the law does not deal with online sales, or specify a requirement to sight ID.	Unclear	Ministry of Health and Social Solidarity
Hungary	1997. évi CLV. Törvény a fogyasztóvédelemről (Act on consumer protection) (Government of Hungary, 1997[300])	**18**	Unclear. The sale of cigarettes to children is prohibited (at §16/A(3)), and proof of age is required at point of sale (at §16/A(4)). However, the law does not deal with online sales.	Unclear	Hungarian Competition Authority
Iceland	Lög um tóbaksvarnir (Tobacco Control Act) (Govermment of Iceland, 2002[331])	**18**	Unclear. The sale of cigarettes to children is prohibited, and proof of age is required at point of sale (at s8). However, the law does not deal with online sales.	Unclear	Ministry of Health
Ireland	Public Health (Tobacco) Act (Government of Ireland, 2002[332])	**18**	Unclear. The sale of cigarettes to children is prohibited, and proof of age is required at point of sale (at s45). However, the law does not deal with online sales.	Unclear	Minister for Health and Children
Israel	Prohibition of Advertising and Restriction of Marketing of		Unclear.	Unclear	Minister of Health

© OECD 2025

Country / Region	Law	Age Limit	Can the good be delivered without a physical ID check?	If yes, what (if any) is the online age assurance requirement?	Administrator
	Tobacco and Smoking Products (Government of Israel, 1983[333])	**18**	The law prohibits the sale of tobacco products (including e-cigarettes) to minors and requires proof of age at point of sale (at art. 8a). The law does not deal with online sales or delivery.		
Italy	REGIO DECRETO 24 dicembre 1934, n. 2316, Approvazione del testo unico delle leggi sulla protezione ed assistenza della maternità ed infanzia (Consolidated text of the laws on the protection and assistance of maternity and childhood) (Government of Italy, 1934[334])	**18**	Unclear. The law prohibits the sale of tobacco products (including e-cigarettes) to persons under the age of 18 and requires proof of age at point of sale if there is doubt about a person's majority (at art. 25). The law does not deal with online sales or delivery.	Unclear	Minister of Health
Japan	Law Concerning the Prohibition of Smoking by Persons Under 20 Years of Age (Government of Japan, 1900[335])	**20**	No. The law prohibits the sale of tobacco products to persons under 20 (at art. 1) and requires proof of age for this purpose (at art. 4). The law does not provide for online sales or delivery, however in practice proof of purchaser's age is also required for online sales.	N/A	National Police Agency
Korea	Youth Protection Act (Government of Korea, 1997[128])	**19**	Unclear. The law defines tobacco as a drug harmful to youth (at art. 2(4)), and prohibits the sale of alcohol to youth, including via communication devices (at art. 28(1)). It requires a seller to verify the age of any purchaser (at art. 28(4)), however it is not clear if this requirement is applicable at point of delivery.	Unclear, while the law prohibits the sale to youth via communication devices, it is not clear if there is an online age assurance requirement for the purpose of enforcing the prohibition.	Ministry of Gender Equality and Family (Youth Protection and Environment Division)
Latvia	Tabakas izstrādājumu, tabakas aizstājējproduktu, augu smēķēšanas produktu, elektronisko smēķēšanas ierīču un to šķidrumu aprites likums (Law on the Handling of Tobacco Products, Tobacco Substitute Products, Herbal Products for	**18**	No. The law prohibits the sale of tobacco products (including e-cigarettes) to children and requires proof of age for this purpose (at art. 8(3)). The law further prohibits the sale of tobacco products using distance communication techniques (at art. 8 (2)).	N/a	Ministry of Health

© OECD 2025

Country / Region	Law	Age Limit	Can the good be delivered without a physical ID check?	If yes, what (if any) is the online age assurance requirement?	Administrator
	Smoking, Electronic Smoking Devices and Their Liquids) (Government of Latvia, 2016[336])				
Lithuania	Lietuvos Respublikos Tabako, Tabako Gaminių Ir Su Jais Susijusių Gaminių Kontrolės Įstatymas (Control of Tobacco, Tobacco Products And Related Products Law) (Government of Lithuania, 1995[337])	**18**	No. The law prohibits the sale of tobacco products (including e-cigarettes) to children and requires proof of age for this purpose (at art. 14(5)(3)). The law further prohibits the sale of tobacco products via distance (at art. 15(1)(2)).	N/a	Ministry of Health
Luxembourg	Loi du 11 août 2006 relative à la lutte antitabac (Law on tobacco control) (Government of Luxembourg, 2006[338])	**16**	Unclear. The law prohibits the sale of tobacco products to persons under 16 (at art. 9). However, the law does not refer to a need for ID checks and does not deal with online sales.	N/A	Ministry of Health
Mexico	Ley General Para El Control Del Tabaco (General Law for Tobacco Control) (Government of Mexico, 2008[339])	**18**	No. The law prohibits the sale of tobacco products to minors and requires proof of age for this purpose (at art. 15). The law further prohibits the sale of tobacco products via "telephone, mail, internet or any other means of communication" (at art. 17). Minors are not defined in this law; however, Mexico's Penal Code defines a minor as persons under 18 (at art. 200) (Government of Mexico, 1931[190]).	N/a	Ministry of Health
Netherlands	Tabaks- en rookwarenwet (Tobacco and Smoking Products Act) (Government of the Netherlands, 1990[340])	**18**	Yes. The law prohibits the sale of tobacco products (including e-cigarettes) to minors and requires an age check for this purpose (at art 8). The law prohibits sales by distance, unless certain safeguards are put in place, including "the use of an age verification system" (at art. 9).	The law does not specify a particular age assurance method for the purpose of complying with article 9.	Minister of Health, Welfare and Sport

© OECD 2025

Country / Region	Law	Age Limit	Can the good be delivered without a physical ID check?	If yes, what (if any) is the online age assurance requirement?	Administrator
New Zealand	Smokefree Environments and Regulated Products Act (Government of New Zealand, 1990[341])	**18**	Yes. The law prohibits the sale of tobaccos products (including e-cigarettes) to persons under 18 (at s40(1)(a)), or having such products delivered to a person under 18 (at s40(1)(b)). Sighting ID is a defense to the offense of selling tobacco products (at s40(4)), however it appears this is only necessary at point of sale, and not at point of delivery.	While the law permits Internet sales and requires age assurance at the point of sale for this purpose, the law does not specify any online age assurance requirement or provide guidance on how age assurance could occur online.	Ministry of Health
Norway	Tobakkssalgsforskriften (Tobacco Sales Regulations) (Government of Norway, 2017[342])	**18**	Unclear. The law prohibits the sale of tobacco products to persons under 18 and requires proof of age for this purpose (at § 3.). The law does not deal with online sales or delivery.	Unclear	Ministry of Health and Care
Poland	Ustawa z dnia 9 listopada 1995 r.o ochronie zdrowia przed następstwami używania tytoniu i wyrobów tytoniowych (Act on the protection of health against the consequences of using tobacco and tobacco products) (Government of Poland, 1995[343])	**18**	No. The law prohibits the sale of tobacco products (including e-cigarettes) to children and requires proof of age for this purpose (at art. 6). The law further prohibits the sale of tobacco products via distance (at art. 7.f).	N/a	Minister of Health.
Portugal	Lei n.º 63/2017 (Law No. 63/2017) (Government of Portugal, 2017[344])	**18**	No. The law prohibits the sale of tobacco products (including e-cigarettes) to children and requires proof of age for this purpose (at art. 15(1)(c)). The law further prohibits the sale of tobacco products via distance or the Internet (at art. 15(1)(d)(e)).	N/a	Ministry of Health
Slovak Republic	ZÁKON z 26. Mája 2004 o ochrane nefajčiarov a o zmene doplnení niektorých zákonov (Law on the Protection of Non-	**18**	Yes. The law prohibits the sale of tobaccos products (including e-cigarettes) to persons under 18 (at Art.1,	While the law permits Internet sales the law does not specify any online age assurance requirement or provide guidance on how age assurance could occur online. The vendor is however required to provide “the Slovak	Slovak Trade Inspection, State Veterinary and Food Administration of the Slovak Republic, and state administration bodies.

© OECD 2025

Country / Region	Law	Age Limit	Can the good be delivered without a physical ID check?	If yes, what (if any) is the online age assurance requirement?	Administrator
	Smokers) (Government of the Slovak Republic, 2004[345])		§6(3)). Distance sales are possible if the vendor institutes an age verification system(Art.1, §6(2)). It is not clear if age verification is necessary at both point of sale and point of delivery.	Trade Inspection with detailed information about the age verification system and its functioning" (at Art.1, §6(2)).	
Slovenia	Zakon o omejevanju uporabe tobačnih izdelkov (Act on the Restriction of the Use of Tobacco and Related Products) (Government of Slovenia, 2017[346])	**18**	No. The law prohibits the sale of tobacco products (including e-cigarettes) to children (at art. 30(1)). The law further prohibits the sale of tobacco products via distance or the Internet (at art. 30(5)).	N/a	Ministry of Health
Spain	Ley 28/2005, de 26 de diciembre, de medidas sanitarias frente al tabaquismo y reguladora de la venta, el suministro, el consumo y la publicidad de los productos del tabaco (Law on health measures against smoking and regulating the sale, supply, consumption and advertising of tobacco products) (Government of Spain, 2006[347])	**18**	No. The law prohibits the sale of tobacco products to children (at art. 3(2)). The law further prohibits the sale of tobacco products via distance (at art. 3(6)).	N/a	General State Administration
Sweden	Lag (2018:2088) om tobak och liknande produkter (Act on Tobacco and Similar Products) (Government of Sweden, 2018[348])	**18**	Yes. The law prohibits the sale of tobaccos products (including e-cigarettes) to persons under 18 and requires an age check for this purpose (at, §17). The requirement to assure age also applies to sales by distances (§18), however it is not clear if age assurance is necessary at both point of sale and point of delivery.	While the law permits distance sales and requires age assurance for this purpose it does not specify how online age assurance should occur.	Ministry of Health and Social Affairs
Switzerland	Loi fédérale sur les produits du tabac et les cigarettes électroniques (Tobacco Products Act) (Government of Switzerland,	**18**	Unclear. The law prohibits the sale of tobacco products (including e-cigarettes) to persons under 18 (at art. 23). The law does not deal with online sales or delivery and has no	Unclear	Competent Cantonal authority/Federal Council

© OECD 2025

Country / Region	Law	Age Limit	Can the good be delivered without a physical ID check?	If yes, what (if any) is the online age assurance requirement?	Administrator
	2024[349])		direct provision of assuring age.		
Türkiye	Tütün Ürünlerinin Zararlarinin Önlenmesi Ve Kontrolü Hakkinda Kanun (Law on the Prevention and Control of the Harms of Tobacco Products) (Government of Türkiye, 1996[350])	**18**	No. The law prohibits the sale of tobacco products to children (at art. 3(8)). The law further prohibits the sale of tobacco products via distance (at art. 3(11)).	N/a	Ministry of Agriculture and Forestry of Turkey
United Kingdom	The Tobacco and Related Products Regulations (Government of the United Kingdom, 2016[351])	**18**	Yes. The Regulation allows cross border distance sales from sellers registered with the Secretary of State (at s47). Such retailers must: • operate an age verification system; and • prior to, or at the time of sale, use that system to confirm the consumers age is not lower than the applicable minimum age. Minimum ages are all 18, however set by different laws in England & Wales (UK Statutory Instruments, 2007[352]), Scotland (Parliament of Scotland, 2010[353])and Northern Ireland (Northern Ireland Statutory Rules, 2008[354]).	The Regulation defines an "age verification system" as "a computing system that confirms the consumer's age electronically" (at s47).	Secretary of State
United States	Title 21, Food and Drugs, cigarettes, smokeless tobacco, and covered tobacco products (Government of the United States, 2010[355])	**21**	Yes. The law prohibits the sale of tobaccos products to persons under 21 and requires an age check for this purpose (at, §1140.14). The law however permits sales by mail order (at § 1140.16) and it is not clear if age assurance for these sales is necessary at either point of sale and point of delivery.	No online age assurance requirement is specified.	Food and Drug Administration

© OECD 2025

Table A E.3. Age limits and age assurance requirements in laws regulating sale of knives

Country / Region	Law	Age Limit	Can the good be delivered without a physical ID check?	If yes, what (if any) is the online age assurance requirement?	Administrator
Australia	Laws differ across states.				
Austria	Waffengesetz (Weapons Act, 1996) (Government of Austria, 1996[356])	**18**	Unclear. The law prohibits the sale of weapons to children (at § 11). While not explicit, the definition of "weapons" likely extends to knives (at § 1). The law does not deal with online sales, or age assurance.	Unclear	District Administrative Authority
Belgium	Loi sur les Armes (Law regulating economic and individual weapons activities) (Government of Belgium, 2006[357])	**18**	No. The law does not expressly prohibit the sale of knives to children, but it does prohibit the sale of weapons (including knives) by mail order or via the Internet (at art. 19(2)).	N/a	Minister of Justice
Canada	Criminal Code (Government of Canada, 1985[358])	**N/a**	Unclear. Canada's Criminal Code bans outright the possession of knives that open automatically (at s 84(1)). The law however does not deal with the sale of knives generally to children.	Unclear.	Minister of Justice
Chile	While Chile has a law dealing with weapons generally (Government of Chile, 1972[359]), this law does not *prima facie* regulate knives, their sale, online purchase, delivery or age assurance.				
Colombia	While Colombia has a law dealing with weapons generally (Government of Colombia, 1993[360]) which *prima facie* deals with knives (at art. 5) the law does not appear to regulate the sale of knives or deal with online purchase / delivery / age assurance.				
Costa Rica	Ley de Armas y Explosivos (Law on Weapons and Explosives) (Government of Costa Rica, 1995[361])	**18**	Unclear. The law prohibits the sale of weapons (including knives) to children (at arts. 3a & 7.c)). However, the law does not deal with online sales or age assurance.	Unclear	Ministry of Public Security
Czechia	While Czechia has a law dealing with weapons generally (Government of Czechia, 2002[362])this law does not *prima facie* regulate knives, their sale, online purchase, delivery or age assurance.				
Denmark	While Denmark has a law dealing with weapons generally (Government of Denmark, 2007[363])this law does not *prima facie* regulate knives, their sale, online purchase, delivery or age assurance.				
Estonia	Relvaseadus (Arms Act)	18	No.	N/A	Estonian Police and Border Guard

© OECD 2025

Country / Region	Law	Age Limit	Can the good be delivered without a physical ID check?	If yes, what (if any) is the online age assurance requirement?	Administrator
	(Government of Estonia, 2002[364])		The law prohibits the sale of weapons to children (at §29)) and requires a permit for their purchase (at§32). It is not clear however which knives would be captured by these provisions.		
Finland	Teräaselaki (Bladed Weapons Act) (Government of Finland, 1997[365])	N/a	No. Finland's law wholly prohibits the sale of "dangerous bladed weapons".	N/a	Minister of Interior
France	Code de la sécurité intérieure (Internal Security Code) (Government of France, 2012[366])	**18**	Unclear. The law prohibits the sale of weapons (which *prima facie* includes knives) to minors (at art R312-1). However, the law does not deal with online sales or age assurance. Minor is not defined in the law however France's Civil Code establishes 18 as the age of majority (at art. 414) (Government of France, 1804[109])	N/A	Minister of Interior
Germany	Waffengesetz (WaffG) (Weapons Act) (Government of Germany, 2002[367])	**18**	Unclear The law prohibits the handling of weapons (including knives) by children (at s2(1)), however more stringent rules relating to licenses do not apply to knives (at s2(2)). The law does not deal with online sales or age assurance.	Unclear	Federal Ministry of the Interior
Greece	While Greece has a law dealing with weapons generally (Government of Greece, 1993[368]) which includes knives (at art. 1) the law does not appear to regulate the sale of knives or that deals with online purchase / delivery / age assurance.				
Hungary	While Hungary has a law dealing with weapons generally (Government of Hungary, 2003[369]) which includes knives (at art. § 4 (1)) the law does not appear to regulate the sale of knives or that deals with online purchase / delivery / age assurance.				
Iceland	While Iceland has a law dealing with weapons generally (Government of Iceland, 1998[370]) which includes knives (at art. 2) the law does not appear to regulate the sale of knives or deal with online purchase / delivery / age assurance.				
Ireland	While Ireland has a law dealing with weapons generally (Government of Ireland, 1990[371]) which includes the possession of knives (at s9) the law does not appear to regulate the sale of knives or deal with online purchase / delivery / age assurance.				
Israel	Penal Code (Government of Israel, 1977[185])	**18**	Unclear. The law prohibits the sale of knives (excluding	Unclear	Minister of Justice

© OECD 2025

Country / Region	Law	Age Limit	Can the good be delivered without a physical ID check?	If yes, what (if any) is the online age assurance requirement?	Administrator
			household knives) to minors and requires proof of age at point of sale (at art. 185). The law does not deal with online sales or delivery.		
Italy	While Italy has a law dealing with weapons generally (Government of Italy, 1931[372])this law does not *prima facie* regulate knives, their sale, online purchase, delivery or age assurance.				
Japan	Act for Controlling the Possession of Firearms or Swords and Other Such Weapons (Government of Japan, 1958[373])	**18**	No. The law requires, in principle, permission must be obtained in advance from the Prefectural Public Safety Commission for the possession of "swords" (including knives, see Article 2.2.) (Article 4) and that persons under 18 years of age may not obtain permission (Article 5.1.1). It also requires that arms manufacturers, etc. shall not transfer (including sale and delivery) swords unless they have taken measures such as obtaining from the transferee a permit evidencing the above-mentioned permission for the possession of the swords (Article 21-2(1)).	N/A	Prefectural Public Safety Commissions
Korea	Act On the Safety Management of Guns, Swords, And Explosives (Government of Korea, 2015[374])	**18**	No. The law prohibits the handling of "swords" (which includes knives) by children (at art. 19) and prohibits their sale the over the internet.	N/a	Ministry of Interior and Safety
Latvia	While Latvia has a law dealing with weapons generally (Government of Latvia, 2019[375])this law does not *prima facie* regulate knives, their sale, online purchase, delivery or age assurance.				
Lithuania	Ginklų Ir Šaudmenų Kontrolės (Arms And Ammunition Control) (Government of Lithuania, 2002[376])	**18**	Unclear. Lithuania's law prohibits outright the possession of certain knives (at art 7), other knives can be purchased by persons over 18 following the "submission of personal documents" (at art. 13.D). It is not clear if this requirement applies to online sales, or if online sales are permissible.	Unclear	Ministry of Interior
Luxembourg	Loi du 15 mars 1983 sur les armes et	**18**	No.	N/a	Minister of Justice

© OECD 2025

Country / Region	Law	Age Limit	Can the good be delivered without a physical ID check?	If yes, what (if any) is the online age assurance requirement?	Administrator
	munitions (Law on arms and ammunition) (Government of Luxembourg, 1983[377])		The law allows purchase of knives only with approval from the Ministry of Justice. And approval is not to be granted to persons under 18 (at art. 13).		
Mexico	While Mexico has a law dealing with weapons generally (Government of Mexico, 1972[378])this law does not *prima facie* regulate knives, their sale, online purchase, delivery or age assurance.				
Netherlands	Wet wapens en munitie (Weapons and Ammunition Act) (Government of the Netherlands, 2017[379])	**18**	Unclear. The law requires authorization for the possession of certain knives (i.e. butterfly knives, folding knives, throwing knives) which can be refused due to age (at art. 10), and other knifes (i.e. other cold weapons with blades) are not able to be possessed by persons under 18. The law however does not deal with age assurance for this purpose, or online sales.	Unclear	Minister of Security and Justice
New Zealand	Summary Offences Act 1981 (Government of New Zealand, 1981[380]) Crimes Act 1961 (Government of New Zealand, 1961[381])	**N/a**	Unclear. New Zealand's criminal law regime outlaws the possession of knives generally. A regulatory Impact Statement from 2010 envisaged a voluntary accord with retailers to limit the sales of knives to young people. However, it is not clear if this occurred. (Government of New Zealand, 2010[382])	Unclear	Ministry of Justice
Norway	While Norway has a law dealing with weapons generally (Government of Norway, 2021[383]) this law does not *prima facie* regulate knives, their sale, online purchase, delivery or age assurance.				
Poland	Ustawa Z Dnia 21 Maja 1999 R. O Broni I Amunicji (Act About Weapons and Ammunition) (Government of Poland, 1999[384])	**N/a**	Unclear The law allows for the purchase of weapons (including knives, see art. 4(1)(4)) via distance and requires a permit for the purchase of certain weapons in this manner. *Prima facie* no permit is required for the purchase of knives. The law does not provide any detail on age limits, or on age assurance for the purpose of online sales.	Unclear	Minister of Health
Portugal	Regime jurídico das armas e suas munições	**N/a**	No.	N/a	National Firearms Center

© OECD 2025

Country / Region	Law	Age Limit	Can the good be delivered without a physical ID check?	If yes, what (if any) is the online age assurance requirement?	Administrator
	(Legal regime of weapons and their ammunition) (Government of Portugal, 2006[385])		The law requires authorisation for the sale of regulated knives (i.e. butterfly knives, folding knives, throwing knives) (at art 3, 4(30). The law, however, is silent on age requirements, and does not deal with online sales		
Slovak Republic	While the Slovak Republic has a law dealing with weapons generally (Government of the Slovak Republic, 2003[386]) this law does not *prima facie* regulate knives, their sale, online purchase, delivery or age assurance.				
Slovenia	Zakon o orožju (Weapons Act) (Government of Slovenia, 2001[387])	**18**	No. The law requires a permit for the purpose of purchasing knives (i.e. daggers, spring daggers) (at arts 3, 4(30) & 14) and specifies that a person must be 18 to obtain a permit. The law however does not deal with online sales.	N/a	Ministry of Interior
Spain	Real Decreto 137/1993, de 29 de enero, por el que se aprueba el Reglamento de Armas (Royal Decree approving the Weapons Regulations) (Government of Spain, 1993[388])	**18**	Unclear. The law prohibits outright the sale and possession of daggers and automatic knives (at art. 4(f)), knives that are not prohibited can be purchased without a license, provided the person is of majority (at art. 106). The law however does not deal with online purchases or age assurance for this purpose. Minor is not defined in the law, however Spain's Civil Code (Government of Spain, 1889[144]) defines the age of majority as 18 (at art 315).	Unclear	Ministry of Interior
Sweden	Förbud beträffande knivar och andra farliga föremål (Act on the prohibition of knives and other dangerous objects) (Government of Sweden, 1988[389])	**21**	Unclear. The law prohibits persons under 21 possessing stabbing weapons or folding knives (at §1), and from being handed spring knives (at §2). The law however does not deal with sales generally, online purchases or age assurance.	Unclear	Ministry of Justice
Switzerland	Loi fédérale sur les armes, accessoires d'armes et munitions	**N/a**	No.	N/a	Federal Council

© OECD 2025

Country / Region	Law	Age Limit	Can the good be delivered without a physical ID check?	If yes, what (if any) is the online age assurance requirement?	Administrator
	(Federal Act on Weapons, Weapon Accessories and Ammunition) (Government of Switzerland, 1997[390])		The law prohibits outright the possession of butterfly knives, throwing knives, and daggers with symmetrical blades (at art. 5).		
Türkiye	Ateşli Silahlar, Bıçaklar ve Diğer Aletlere İlişkin Yönetmelik (Regulation Regarding Firearms, Knives and Other Tools) (Government of Türkiye, 1991[391])	**N/a**	Unclear. The law includes knives as a regulated weapon (at art. 2(i)), however only deals with requirements for the purchase from persons you use them for their craft or profession (at art. 53). The law does not specify an age limit or provide any details on online sales.	N/a	Ministry of Interior
United Kingdom	Criminal Justice Act (Section 141) (Government of the United Kingdom, 1988[392])	**18**	Yes. The law prohibits the sale of a "knife, knife blade or razor blade (…) and any other article which has a blade" to persons under 18. It is a defense to "take all reasonable precautions" however, it is not specified if this includes assuring age. Online sales are permitted and a voluntary agreement between the UK Government and major retailers, provides that age assurance must occur at point of delivery, including for online retailers. Online retailers who do not do this, face suspension (Government of the United Kingdom, 2024[393]).	While there is an agreement requiring age assurance at point of delivery this is unenforceable.	Trading Standards departments of local authorities
United States	Laws differ across states.				

© OECD 2025

References

5Rights Foundation (2021), *But how do they know it is a child? Age Assurance in the Digital World*, https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf. [16]

Age Assurance Technology Trial (2025), *Evaluating the effectiveness, maturity and readiness of age assurance for Australia*, https://ageassurance.com.au/. [47]

Age Verification Providers Association (2025), *International Standards for Age Verification*, https://avpassociation.com/standards-for-age-verification/. [33]

Age Verification Providers Association (2025), *Overview of Members' services*, https://avpassociation.com/find-an-av-provider/. [32]

Agencia Española de Protección de Datos (2024), *Technical Note: A safe internet for children and the role of age verification*, https://www.aepd.es/guides/technical-note-safe-internet-by-default-for-children.pdf. [87]

Agencia Española de Protección de Datos (2023), *Decalogue of Principles: Age verification and protection of minors from inappropriate content*, https://www.aepd.es/guides/decalogue-principles-age-verification-minors-protection.pdf. [84]

Agencia Española de Protección de Datos (2023), *Technical Note: Description of the proofs of systems for age verification and protection of minors from inappropriate content*, https://www.aepd.es/guides/technical-note-proof-of-concept-age-verification-systems.pdf. [85]

Alabama State Legislature (2024), *House Bill 164*, https://legiscan.com/AL/bill/HB164/2024. [199]

Alabama State Legislature (1975), *Code of Alabama*, https://casetext.com/statute/code-of-alabama/title-13a-criminal-code/chapter-12-offenses-against-public-health-and-morals/article-4-obscenity-and-related-offenses/division-5-alabama-anti-obscenity-enforcement-act/section-13a-12-2001-definitions. [200]

Alcohol and Drug Foundation (2024), *The rise of online alcohol delivery*, https://cdn.adf.org.au/media/documents/MB_OnlineAlcoholDelivery.pdf. [57]

Apple (2024), *Apple Developer - Age ratings*, https://developer.apple.com/help/app-store-connect/reference/age-ratings. [72]

Apple (2024), *Apple Developer - Set an app age rating*, https://developer.apple.com/help/app-store-connect/manage-app-information/set-an-app-age-rating. [71]

ARCOM (2023), *La fréquentation des sites "adultes" par les mineurs*, https://www.arcom.fr/nos-ressources/etudes-et-donnees/mediatheque/frequentation-des-sites-adultes-par-les-mineurs. [40]

© OECD 2025

Arcom (2025), *Pornographie en ligne : de nouvelles étapes franchies pour la protection des mineurs*, https://www.arcom.fr/presse/pornographie-en-ligne-de-nouvelles-etapes-franchies-pour-la-protection-des-mineurs. [50]

Arcom (2024), *Référentiel technique sur la vérification de l'âge pour la protection des mineurs contre la pornographie en ligne*, https://www.arcom.fr/se-documenter/espace-juridique/textes-juridiques/referentiel-technique-sur-la-verification-de-lage-pour-la-protection-des-mineurs-contre-la-pornographie-en-ligne. [110]

Arkansas State Senate (2023), *The Protection of Minors from Distribution of Harmful Material Act (Senate Bill 66)*, https://www.arkleg.state.ar.us/Bills/Detail?id=sb66&ddBienniumSession=2023%2F2023R#:~:text=SB66%20%2D%20TO%20CREATE%20THE%20PROTECTION,TO%20REQUIRE%20REASONABLE%20AGE%20VERIFICATION. [201]

Australian eSafety Commissioner (2022), *Age Verification*, https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification. [17]

Australia's eSafety Commissioner (2025), *Social Media Age Restrictions*, https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions. [46]

Australia's eSafety Commissioner (2024), *eSafety position paper: Development of Phase 2 industry codes*, https://www.esafety.gov.au/sites/default/files/2024-07/Development-of-Phase-2-Industry-Codes-under-the-Online-Safety-Act-eSafety-position-paper_0.pdf?v=1727970412207. [38]

Australia's eSafety Commissioner (2024), *Industry Codes and Standards*, https://www.esafety.gov.au/industry/codes. [91]

Australia's eSafety Commissioner (2024), *Statement: announcement of age assurance trial*, https://www.esafety.gov.au/newsroom/media-releases/statement-announcement-of-age-assurance-trial. [48]

Australia's eSafety Commissioner (2023), *Phase 1 Industry Codes (Class 1A and 1B Material) Regulatory Guidance*, https://www.esafety.gov.au/sites/default/files/2023-12/Phase-1-Industry-Codes-%28Class-1A-and-Class-1B-Material%29-Regulatory-Guidance.pdf. [92]

Biometric Update (2025), *Age check legislation to prevent youth alcohol, tobacco sales expanding globally*, https://www.biometricupdate.com/202502/age-check-legislation-to-prevent-youth-alcohol-tobacco-sales-expanding-globally. [58]

British Board of Film Classification (2020), *Young people, Pornography & Age-verification*, https://revealingreality.co.uk/wp-content/uploads/2020/01/BBFC-Young-people-and-pornography-Final-report-2401.pdf. [51]

Bundesprüfstelle für jugendgefährdende Medien (2024), *Was wird indiziert?*, https://www.bzkj.de/bzkj/indizierung/was-wird-indiziert. [113]

California State Legislature (2024), *Protecting Our Kids from Social Media Addiction Act (SB 976)*, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240SB976. [162]

Canada Office of the Privacy Commissioner (2024), *Privacy and age assurance – Exploratory consultation*, https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-age/expl_gd_age/. [86]

© OECD 2025

Canadian Broadcast Standards Council (2024), *Ratings Classification*, https://www.cbsc.ca/tools/ratings-classifications/. [175]

Canadian Centre for Child Protection (2022), *Reviewing the Enforcement of App Age Ratings in Apple's App Store and Google Play*, https://protectchildren.ca/en/resources-research/app-age-ratings-report/. [75]

CELE (2019), *Colombia draft law regulation of use and appropriation of social networks*, https://observatoriolegislativocele.com/en/Colombia-draft-law-regulation-of-use-and-appropriation-of-social-networks-2019/#:~:text=To%20ensure%20the%20proper%20use,express%20consent%20of%20their%20parents. [158]

Centre for Information Policy Leadership (2024), *About us*, https://www.informationpolicycentre.com/about.html. [394]

CIPL / WeProtect (2024), *A Multi-Stakeholder Dialogue on Age Assurance: Key Takeaways*, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/key_takeaways_from_a_multi-stakeholder_dialogue_on_age_assurance.pdf. [27]

CNIL (2021), *Recommandation 7 : vérifier l'âge de l'enfant et l'accord des parents dans le respect de sa vie privée*, https://www.cnil.fr/fr/recommandation-7-verifier-lage-de-lenfant-et-laccord-des-parents-dans-le-respect-de-sa-vie-privee. [244]

Coimisiún na Meán (2025), *Online Safety Code*, http://Online Safety Code. [124]

Coimisiún na Meán (2024), *Draft Online Safety Code*, https://www.cnam.ie/wp-content/uploads/2024/05/Online-Safety-Code_vFinal.pdf. [43]

Colorado State Legislature (2024), *Healthier Social Media Use by Youth (HB24-1136)*, https://leg.colorado.gov/bills/hb24-1136. [163]

Comisión de Regulación de Comunicaciones (2016), *Resolución 5050 de 2016*, https://gestornormativo.creg.gov.co/gestor/entorno/docs/resolucion_crc_5050_2016.htm. [177]

Commission Nationale de l'Informatique et des Libertés (2022), *Demonstration of a privacy-preserving age verification process*, https://linc.cnil.fr/demonstration-privacy-preserving-age-verification-process. [82]

Commission Nationale de l'Informatique et des Libertés (2022), *Online age verification: balancing privacy and the protection of minors*, https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors. [83]

Committee on the Rights of the Child (2021), *General Comment no. 25 on children's rights in relation to the digital environment*, https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation. [25]

Council of Europe (2018), *Guidelines to respect, protect and fulfil the rights of the child in the digital environment*, https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a. [26]

Danish Media Council for Children and Young People (2025), *Ethical Guidelines for Digital Service Providers*, https://digitaletik.dk/. [101]

Digital Trust and Safety Partnership (2023), *Age Assurance: Guiding Principles and Best* [28]

© OECD 2025

Practices, https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.

ESRB (2025), *About the ESRB*, https://www.esrb.org/. [63]

ESRB (2025), *Our history*, https://www.esrb.org/history/. [61]

ESRB (2024), *Frequently asked questions*, https://www.esrb.org/faqs/#are-all-games-required-to-have-a-rating. [64]

European Audiovisual Observatory (2024), *AGCOM public consultation on the methods of verification of the age of majority by website managers and video-sharing platform suppliers*, https://merlin.obs.coe.int/article/10035. [42]

European Audiovisual Observatory (2023), *The protection of minors on VSPs: age verification and parental control*, https://rm.coe.int/the-protection-of-minors-on-vsps-age-verification-and-parental-control/1680af0788. [36]

European Commission (2024), *Commission launches call for evidence for guidelines on protection of minors online under the Digital Services Act*, https://digital-strategy.ec.europa.eu/en/news/commission-launches-call-evidence-guidelines-protection-minors-online-under-digital-services-act. [37]

European Commission (2024), *Digital Services Act: Task Force on Age Verification*, https://digital-strategy.ec.europa.eu/en/news/digital-services-act-task-force-age-verification-0. [45]

European Commission (2022), *A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+)*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:212:FIN#footnote4. [103]

European Commission (2022), *Digital Services Act*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065. [35]

European Commission (2018), *Audiovisual Media Services Directive*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02010L0013-20181218. [34]

European Commission (2016), *Regulation (EU) 2016/679 of the European Parliament and of the Council of 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 (GDPR)*, https://eur-lex.europa.eu/eli/reg/2016/679/oj. [241]

European Commission (2015), *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366. [307]

European Data Protection Board (2025), *Statement 1/2025 on Age Assurance*, https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/statement-12025-age-assurance_en. [89]

European Union (2025), *Glossary of summaries: Transposition*, https://eur-lex.europa.eu/EN/legal-content/glossary/transposition.html#:~:text=Transposition%20is%20the%20process%20of,laws%20of%20EU%20Member%20States. [49]

European Union (2014), *Tobacco Products Directive (2014/40/EU)*, [402]

© OECD 2025

https://health.ec.europa.eu/document/download/c4aa6f75-7e52-463b-badb-cbb6181b87c3_en?filename=dir_201440_en.pdf.

Florida State Legislature (2024), *An act relating to online protections for minors (HB 3)*, https://www.flsenate.gov/Session/Bill/2024/3. [164]

Florida State Legislature (2024), *The Florida Statues*, http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0800-0899/0827/Sections/0827.071.html#:~:text=(a)%20%E2%80%9CChild%E2%80%9D%20or,than%2018%20years%20of%20age. [202]

Fraunhofer IDMT (2025), *IDCheck – AI-based identity verification*, https://www.idmt.fraunhofer.de/en/institute/projects-products/idcheck-identity-verification.html. [115]

Free Speech Coalition (2025), *2024 Age-Verification Legislative Scorecard*, https://action.freespeechcoalition.com/status-update-state-age-verification-legislation/. [14]

Game Rating and Administration Committee (2025), *About GRAC*, https://www.grac.or.kr/english/. [69]

Games Rating Authority (2024), *Our History*, https://gamesratingauthority.org.uk/RatingBoard/about-history. [60]

Games Rating Authority (2024), *PEGI Ratings*, https://gamesratingauthority.org.uk/RatingBoard/ratings. [73]

Georgia State Legislature (2024), *Protecting Georgia's Children on Social Media Act of 2024 (SB 351)*, https://www.billtrack50.com/billdetail/1672658. [165]

Global Online Safety Regulators Network (2024), *Position Statement, Regulatory coherence and coordination: the role of the Global Online Safety Regulators Network*, https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/other/gosrn-position-statement-on-regulatory-coherence.pdf?v=361088. [30]

Govermment of Iceland (2002), *Lög um tóbaksvarnir*, https://www.althingi.is/lagas/154b/2002006.html. [331]

Government of Australia (2025), *Australian Classification*, https://www.classification.gov.au/. [67]

Government of Australia (2024), *Online Safety Amendment (Social Media Minimum Age) Act*, https://www.legislation.gov.au/C2024A00127/asmade/text. [156]

Government of Australia (2023), *Social Media Online Safety Code (Class 1A and 1B Material)*, https://www.esafety.gov.au/sites/default/files/2023-06/Schedule-1%E2%80%93Social-Media-Services-Online-Safety-Code-%28Class-1A-and-Class-1B-Material%29.pdf. [157]

Government of Australia (2021), *Online Safety Act*, https://www.legislation.gov.au/C2021A00076/latest/text. [90]

Government of Australia (2013), *National Classification Code*, https://www.legislation.gov.au/F2005L01284/latest/text. [174]

Government of Australia (1988), *The Privacy Act (Cth)*, https://www.legislation.gov.au/C2004A03712/latest/versions. [227]

© OECD 2025

Government of Austria (2024), *Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Datenschutzgesetz*, https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597. [229]

Government of Austria (2024), *Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Tabak- und Nichtraucherinnen- bzw. Nichtraucherschutzgesetz*, https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10010907. [325]

Government of Austria (2020), *Audiovisuelle Mediendienste-Gesetz*, https://www.jusline.at/gesetz/amd-g. [93]

Government of Austria (2018), *ABGB - Allgemeines bürgerliches Gesetzbuch*, https://www.jusline.at/gesetz/abgb/paragraf/21. [94]

Government of Austria (1996), *Waffengesetz*, https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10006016. [356]

Government of Belgium (2018), *Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*, https://etaamb.openjustice.be/fr/loi-du-30-juillet-2018_n2018040581.html. [230]

Government of Belgium (2017), *Loi relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale*, https://www.ejustice.just.fgov.be/eli/loi/2017/05/05/2017040323/justel. [95]

Government of Belgium (2006), *Loi sur les Armes*, https://www.ejustice.just.fgov.be/cgi/article_body.pl?language=fr&caller=summary&pub_date=2006-06-09&numac=2006009449. [357]

Government of Belgium (1997), *Loi relative à la protection de la santé des consommateurs en ce qui concerne les denrées alimentaires et les autres produits*, https://www.ejustice.just.fgov.be/eli/loi/1977/01/24/1977012405/justel. [288]

Government of Belgium (1804), *Code Civile*, https://www.ejustice.just.fgov.be/cgi_loi/article.pl?language=fr&sum_date=&pd_search=1807-09-03&numac_search=1804032150&page=2&lg_txt=F&caller=list&1804032150=4&trier=promulgation&view_numac=1804032130fr&dt=CODE+CIVIL&fr=f&choix1=ET#LNK0157. [96]

Government of Canada (2000), *Personal Information Protection and Electronic Documents Act*, https://laws-lois.justice.gc.ca/eng/acts/p-8.6/index.html. [231]

Government of Canada (1985), *Criminal Code*, https://laws-lois.justice.gc.ca/PDF/C-46.pdf. [358]

Government of Chile (2024), *Ley Sobre Expendio y Consumo de Bebidas Alcoholicas*, https://www.bcn.cl/leychile/navegar?idNorma=220208. [289]

Government of Chile (2016), *Normas Generales sobre Contenidos de las Emisiones de Televisión*, https://www.bcn.cl/leychile/navegar?idNorma=1089666. [176]

Government of Chile (1999), *Sobre Proteccion de la Vida Privada (Ley 19628)*, [234]

© OECD 2025

https://www.bcn.cl/leychile/navegar?idNorma=141599.

Government of Chile (1995), *Ley 19419 Regula Actividades Que Indica Relacionadas Con El Tabaco*, https://www.bcn.cl/leychile/navegar?idNorma=30786&idVersion=2022-02-01&idParte=10483958. [326]

Government of Chile (1972), *Ley 17798 Establece el control de armas*, https://www.bcn.cl/leychile/navegar?idNorma=29291. [359]

Government of Colombia (2021), *Proyecto de Ley No. 600 de 2021 Cámara*, https://www.camara.gov.co/audiencia-publica-proyecto-de-ley-no-600-de-2021-camara. [79]

Government of Colombia (2013), *Decree no. 1377 of 2013*, https://www.littler.com/files/press/related-files/DECRETO%201377%20DEL%2027%20DE%20JUNIO%20DE%202013%20(2)%20(2).pdf. [236]

Government of Colombia (2012), *Ley no. 1581 of 2012 por la cual se dictan disposiciones generales para la protección de datos personales*, https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1684507. [235]

Government of Colombia (2010), *Decree 120 of 2010 National Level*, https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=38680#0. [291]

Government of Colombia (2009), *Ley Número 1335 De 2009*, https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/DE/DIJ/Ley%201335%20de%202009.pdf. [327]

Government of Colombia (2006), *Por la cual se expide el Código de la Infancia y la Adolescencia (Ley 1098 de 2006)*, https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1673639. [178]

Government of Colombia (1994), *Ley 124 de 1994 por la cual se prohíbe el expendio de bebidas embriagantes a menores de edad y se dictan otras disposiciones*, https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=291. [290]

Government of Colombia (1993), *Decreto 2535 de 1993 por el cual se expiden normas sobre armas, municiones y explosivos*, https://www.suin-juriscol.gov.co/viewDocument.asp?id=1461503. [360]

Government of Costa Rica (2021), *Reforma integral a La Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales*, https://delfino.cr/asamblea/proyecto/22388. [80]

Government of Costa Rica (2012), *Ley General De Control Del Tabaco Y Sus Efectos Nocivos En La Salud*, http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=72249. [328]

Government of Costa Rica (2011), *Ley de Protección de la Persona frente al tratamiento de sus datos personales (No. 8968)*, http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&strTipM=TC. [237]

Government of Costa Rica (2011), *Protección de la niñez y la adolescencia frente al contenido* [179]

© OECD 2025

nocivo de internet y otros medios electrónicos (Ley no. 8934, http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=71024&nValor3=86030&param2=1&strTipM=TC&lResultado=2&strSim=simp.

Government of Costa Rica (1996), *Regulación De Horarios De Funcionamiento En Expendios De Bebidas Alcohólicas*, http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=42514. [292]

Government of Costa Rica (1995), *Ley de Armas y Explosivos*, http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=26048. [361]

Government of Costa Rica (1985), *Código Civil*, http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=15437. [180]

Government of Czechia (2022), *Zákon o službách platforem pro sdílení videonahrávek a o změně některých souvisejících zákonů (zákon o službách platforem pro sdílení videonahrávek*, https://www.zakonyprolidi.cz/cs/2022-242. [97]

Government of Czechia (2019), *Zákon o ochraně osobních údajů*, https://www.zakonyprolidi.cz/cs/2019-110. [238]

Government of Czechia (2017), *Zákon č. 65/2017 Sb. Zákon o ochraně zdraví před škodlivými účinky návykových látek*, https://www.zakonyprolidi.cz/cs/2017-65. [293]

Government of Czechia (2012), *Zákon č. 89/2012 Sb. Zákon občanský zákoník*, https://www.zakonyprolidi.cz/cs/2012-89. [98]

Government of Czechia (2002), *Předpis č. 119/2002 Sb., zdroj: Sbírka zákonů ročník*, https://www.sagit.cz/info/sb02119. [362]

Government of Denmark (2021), *Straffeloven*, https://www.retsinformation.dk/eli/lta/2021/1851. [181]

Government of Denmark (2020), *Bekendtgørelse om videodelingsplatformstjeneste*, https://www.retsinformation.dk/eli/lta/2020/1158. [99]

Government of Denmark (2018), *Databeskyttelsesloven*, https://www.retsinformation.dk/eli/lta/2018/502. [239]

Government of Denmark (2008), *Herved bekendtgøres lov om forbud mod salg af tobak og alkohol til personer under 18*, https://www.retsinformation.dk/eli/lta/2019/964. [294]

Government of Denmark (2007), *Bekendtgørelse af lov om våben og eksplosivstoffer m.v.*, https://www.retsinformation.dk/eli/lta/2021/1736. [363]

Government of Denmark (2007), *Bekendtgørelse af værgemålsloven*, https://www.retsinformation.dk/eli/lta/2007/1015. [100]

Government of Estonia (2018), *Isikuandmete kaitse seadus*, https://www.riigiteataja.ee/akt/104012019011. [240]

Government of Estonia (2014), *Lastekaitseseadus*, https://www.riigiteataja.ee/akt/LasteKS. [183]

© OECD 2025

Government of Estonia (2010), *Meediateenuste seadus*, https://www.riigiteataja.ee/akt/106012011001?leiaKehtiv. [102]

Government of Estonia (2005), *Tubakaseadus*, https://www.riigiteataja.ee/akt/TubS. [329]

Government of Estonia (2002), *Alkoholiseadus*, https://www.riigiteataja.ee/akt/832173. [295]

Government of Estonia (2002), *Relvaseadus*, https://www.riigiteataja.ee/akt/RelvS. [364]

Government of Estonia (2001), *Karistusseadustik*, https://www.riigiteataja.ee/akt/104072024025. [182]

Government of Finland (2024), *Request for comments on the draft Government proposal to Parliament for an act amending the Alcohol Act*, https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=b56fc88d-7890-4ed3-95a9-04337b035db1. [297]

Government of Finland (2018), *Tietosuojalaki*, https://www.finlex.fi/fi/laki/ajantasa/2018/20181050. [242]

Government of Finland (2017), *Alkoholilaki*, https://www.finlex.fi/fi/laki/ajantasa/2017/20171102. [296]

Government of Finland (2016), *Tobakslag*, https://www.finlex.fi/sv/laki/ajantasa/2016/20160549#P120. [330]

Government of Finland (2011), *Kuvaohjelmalaki*, https://finlex.fi/fi/laki/ajantasa/2011/20110710. [104]

Government of Finland (1999), *Laki holhoustoimesta*, https://www.finlex.fi/fi/laki/ajantasa/1999/19990442. [105]

Government of Finland (1997), *Teräaselaki*, https://www.finlex.fi/fi/laki/alkup/1977/19770108. [365]

Government of France (2024), *LOI n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique*, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000049563368/. [107]

Government of France (2012), *Code de la sécurité intérieure*, https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000025503132/LEGISCTA000025505621/#LEGISCTA000034114975. [366]

Government of France (1986), *Law No. 86-1067 of September 30, 1986 relating to freedom of communication (Léotard Law)*, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000512205/2024-10-07/. [106]

Government of France (1978), *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/. [243]

Government of France (1953), *Code de la santé publique*, https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038369305. [298]

Government of France (1810), *Code Pénal*, https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000044394218. [108]

Government of France (1804), *Code civil*, https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070721/LEGISCTA000006089697/#LEGISCTA000006089697. [109]

Government of Germany (2018), *Bundesdatenschutzgesetz (BDSG)*, https://www.gesetze-im- [245]

© OECD 2025

internet.de/bdsg_2018/BJNR209710017.html#BJNR209710017BJNG001900000.

Government of Germany (2002), *Jugendschutzgesetz (JuSchG)*, https://www.gesetze-im-internet.de/juschg/JuSchG.pdf. [112]

Government of Germany (2002), *Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien*, https://www.gesetze-bayern.de/Content/Document/JMStV. [111]

Government of Germany (2002), *Waffengesetz*, https://www.gesetze-im-internet.de/englisch_waffg/englisch_waffg.html#p0023. [367]

Government of Greece (2021), *Law 4779 of 2021*, https://www.kodiko.gr/nomothesia/document/672722/nomos-4779-2021. [116]

Government of Greece (2019), *Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data*, https://www.dpa.gr/sites/default/files/2020-08/LAW%204624_2019_EN_TRANSLATED%20BY%20THE%20HDPA.PDF. [246]

Government of Greece (2008), *Protection of minors from tobacco and alcoholic beverages and other provisions*, https://www.kodiko.gr/nomothesia/document/141125/nomos-3730-2008. [299]

Government of Greece (1993), *Regulation of matters relating to weapons, ammunition, explosives, explosive devices and other provisions (Government of Greece, 1993[306])*, https://www.kodiko.gr/nomothesia/document/222364/nomos-2168-1993. [368]

Government of Greece (1946), *Civil Code*, https://www.ministryofjustice.gr/wp-content/uploads/2019/10/%CE%91%CF%83%CF%84%CE%B9%CE%BA%CF%8C%CF%82-%CE%9A%CF%8E%CE%B4%CE%B9%CE%BA%CE%B1%CF%82.pdf. [117]

Government of Hungary (2024), *Act CXII of 2011 on the right to informational self determination and on the freedom of information*, https://njt.hu/jogszabaly/en/2011-112-00-00. [247]

Government of Hungary (2016), *Digital Child Protection Strategy*, https://2015-2019.kormany.hu/download/f/3b/21000/The%20Digital%20Child%20Protection%20Strategy%20of%20Hungary.pdf. [120]

Government of Hungary (2013), *2013. évi V. törvény a Polgári Törvénykönyvről*, https://net.jogtar.hu/jogszabaly?docid=A1300005.TV&searchUrl=/gyorskereso?keyword%3Dgyermek. [119]

Government of Hungary (2003), *Korm. rendelet a közbiztonságra különösen veszélyes eszközökről*, https://net.jogtar.hu/jogszabaly?docid=A0300175.KOR. [369]

Government of Hungary (2001), *2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről*, https://net.jogtar.hu/jogszabaly?docid=a0100108.tv. [118]

Government of Hungary (1997), *1997. évi CLV. Törvény a fogyasztóvédelemről*, https://net.jogtar.hu/jogszabaly?docid=99700155.tv. [300]

Government of Hungary (1997), *1997. évi XXXI. törvény a gyermekek védelméről és a gyámügyi igazgatásról*, https://net.jogtar.hu/jogszabaly?docid=99700031.TV&searchUrl=/gyorskereso?keyword%3Dg [184]

© OECD 2025

yermekv%25C3%25A9delem.

Government of Iceland (2018), *Lög um persónuvernd og meðferð persónuupplýsinga*, https://www.althingi.is/lagas/nuna/2018090.html. [248]

Government of Iceland (2011), *Lög um fjölmiðla*, https://www.althingi.is/lagas/nuna/2011038.html. [121]

Government of Iceland (1998), *Áfengislög*, https://www.althingi.is/altext/stjt/1998.075.html. [301]

Government of Iceland (1998), *Vopnalög*, https://www.althingi.is/lagas/nuna/1998016.html. [370]

Government of Iceland (1997), *Lögræðislög*, https://www.althingi.is/lagas/nuna/1997071.html. [122]

Government of Ireland (2022), *Online Safety and Media Regulation Act*, https://www.oireachtas.ie/en/bills/bill/2022/6/. [123]

Government of Ireland (2022), *Online Safety and Media Regulation Act*, https://www.irishstatutebook.ie/eli/2022/act/41/section/45/enacted/en/html#sec45. [160]

Government of Ireland (2018), *Data Protection Act*, https://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html. [249]

Government of Ireland (2002), *Public Health (Tobacco) Act*, https://www.irishstatutebook.ie/eli/2002/act/6/enacted/en/html. [332]

Government of Ireland (1990), *Fireams and Offensive Weapons Act*, https://revisedacts.lawreform.ie/eli/1990/act/12/revised/en/html. [371]

Government of Ireland (1988), *Intoxicating Liquor Act*, https://www.irishstatutebook.ie/eli/1988/act/16/enacted/en/print.html. [302]

Government of Israel (1983), *Prohibition of Advertising and Restriction of Marketing of Tobacco and Smoking Products, 5743-1983*, https://www.nevo.co.il/law_html/law00/71594.htm. [333]

Government of Israel (1981), *Protection of Privacy Law (no. 5741-1981)*, https://www.nevo.co.il/law_html/law00/71631.htm. [251]

Government of Israel (1977), *Penal Code*, https://www.nevo.co.il/law_html/law01/073_002.htm#Seif440. [185]

Government of Israel (1962), *Legal Capacity and Guardianship Law*, https://www.nevo.co.il/law_html/law00/70325.htm. [252]

Government of Italy (2021), *Decreto Legislativo 8 novembre 2021, n. 208*, https://www.gazzettaufficiale.it/eli/id/2021/12/10/21G00231/sg. [125]

Government of Italy (2003), *Codice in materia di protezione dei dati personali*, https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali+%28Testo+coordinato%29. [253]

Government of Italy (2001), *Legge 30 marzo 2001, n. 125, Legge quadro in materia di alcol e di problemi alcolcorrelati*, https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2001;125. [303]

Government of Italy (1942), *Civil Code*, https://www.normattiva.it/esporta/attoCompleto?atto.dataPubblicazioneGazzetta=1942-04- [126]

© OECD 2025

04&atto.codiceRedazionale=042U0262.

Government of Italy (1934), *REGIO DECRETO 24 dicembre 1934, n. 2316, Approvazione del testo unico delle leggi sulla protezione ed assistenza della maternità ed infanzia*, https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:regio.decreto:1934-12-24;2316. [334]

Government of Italy (1931), *Testo unico delle leggi di pubblica sicurezza*, https://www.ce.camcom.it/sites/default/files/contenuto_redazione/allegati/rd773_31.pdf. [372]

Government of Japan (2025), *Cabinet Order No. 507 of 15: Enforcement Order of the Act on the Protection of Personal Information*, https://laws.e-gov.go.jp/law/415CO0000000507/. [257]

Government of Japan (2008), *Act on Establishment of Enhanced Environment for Youth's Safe and Secure Internet Use*, https://laws.e-gov.go.jp/law/420AC1000000079. [127]

Government of Japan (2003), *Act on the Protection of Personal Information (Act No. 57 of 2003)*, https://laws.e-gov.go.jp/law/415AC0000000057. [254]

Government of Japan (1958), *Firearms and Swords Possession Control Law*, https://laws.e-gov.go.jp/law/333AC0000000006#Mp-Ch_2-At_4. [373]

Government of Japan (1922), *Law concerning the prohibition of drinking by persons under the age of 20*, https://laws.e-gov.go.jp/law/211AC1000000020. [304]

Government of Japan (1908), *Criminal Code*, https://laws.e-gov.go.jp/law/140AC0000000045#Mp-Pa_2-Ch_22. [186]

Government of Japan (1900), *Law Concerning the Prohibition of Smoking by Persons Under 20 Years of Age*, https://laws.e-gov.go.jp/law/133AC1000000033. [335]

Government of Korea (2025), *Notification on the Electronic Transaction of Alcoholic Beverages*, https://www.law.go.kr/%ED%96%89%EC%A0%95%EA%B7%9C%EC%B9%99/%EC%A3%BC%EB%A5%98%EC%9D%98%20%ED%86%B5%EC%8B%A0%ED%8C%90%EB%A7%A4%EC%97%90%20%EA%B4%80%ED%95%9C%20%EB%AA%85%EB%A0%B9%EC%9C%84%EC%9E%84%20%EA%B3%A0%EC%8B%9C. [305]

Government of Korea (2023), *Personal Information Protection Act*, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%B2%95. [258]

Government of Korea (2015), *Act On the Safety Management of Guns, Swords, And Explosives*, https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=50961&type=new&key=. [374]

Government of Korea (2001), *Act on Promotion of Information and Communications Network Utilisation and Information Protection*, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EB%A7%9D%EC%9D%B4%EC%9A%A9%EC%B4%89%EC%A7%84%EB%B0%8F%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%93%B1%EC%97%90%EA%B4%80%ED%95%9C%EB%B2%95%EB%A5%A0. [130]

Government of Korea (1997), *Enforcement Decree of the Youth Protection Act*, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%B2%AD%EC%86%8C%EB%85%84%EB%B3%B4%ED%98%B8%EB%B2%95%EC%8B%9C%ED%96%89%EB%A0%B9. [129]

Government of Korea (1997), *Youth Protection Act*, [128]

© OECD 2025

https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%B2%AD%EC%86%8C%EB%85%84%EB%B3%B4%ED%98%B8%EB%B2%95.

Government of Korea (1953), *Penal Code*, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%ED%98%95%EB%B2%95. [187]

Government of Latvia (2019), *Ieroču aprites likums*, https://likumi.lv/ta/en/en/id/305818-law-on-the-handling-of-weapons. [375]

Government of Latvia (2018), *Fizisko personu datu apstrādes likums*, https://likumi.lv/ta/id/300099-fizisko-personu-datu-apstrades-likums. [260]

Government of Latvia (2016), *Tabakas izstrādājumu, tabakas aizstājējproduktu, augu smēķēšanas produktu, elektronisko smēķēšanas ierīču un to šķidrumu aprites likums*, https://likumi.lv/ta/en/en/id/282077-law-on-the-handling-of-tobacco-products-tobacco-substitute-products-herbal-products-for-smoking-electronic-smoking-devices-and-their-liquids. [336]

Government of Latvia (2010), *Elektronisko plašsaziņas līdzekļu likums*, https://likumi.lv/ta/id/214039-elektronisko-plassazinas-lidzeklu-likums. [131]

Government of Latvia (2004), *Alkoholisko dzērienu aprites likums*, https://likumi.lv/ta/en/en/id/88009. [306]

Government of Latvia (1998), *Bērnu tiesību aizsardzības likums*, https://likumi.lv/ta/id/49096-bernu-tiesibu-aizsardzibas-likums. [188]

Government of Lithuania (2002), *Ginklų Ir Šaudmenų Kontrolės*, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.159542. [376]

Government of Lithuania (2000), *Lietuvos Respublikos civilinis kodekas*, https://www.infolex.lt/ta/20799. [133]

Government of Lithuania (1996), *Lietuvos respublikos Asmens duomenų teisinės apsaugos Įstatymas*, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.29193/asr. [261]

Government of Lithuania (1996), *Lietuvos Respublikos visuomenės informavimo įstatymas*, https://www.e-tar.lt/portal/lt/legalAct/TAR.065AB8483E1E/asr. [132]

Government of Lithuania (1995), *Alkoholio Kontrolės Įstatymas*, https://www.e-tar.lt/portal/en/legalAct/TAR.9E5C5C16B6E6/PHqiQkbzfM. [308]

Government of Lithuania (1995), *Lietuvos Respublikos Tabako, Tabako Gaminių Ir Su Jais Susijusių Gaminių Kontrolės Įstatymas*, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.24500/asr. [337]

Government of Luxembourg (2018), *Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données*, https://legilux.public.lu/eli/etat/leg/loi/2018/08/01/a686/jo. [262]

Government of Luxembourg (2006), *Loi du 11 août 2006 relative à la lutte antitabac*, https://legilux.public.lu/eli/etat/leg/loi/2006/08/11/n1/jo#art_9. [338]

Government of Luxembourg (2006), *Loi du 22 décembre 2006 portant interdiction de la vente de boissons alcooliques à des mineurs de moins de seize ans*, https://legilux.public.lu/eli/etat/leg/loi/2006/12/22/n11/jo. [309]

© OECD 2025

Government of Luxembourg (1991), *Loi du 27 juillet 1991 sur les médias électroniques*, https://legilux.public.lu/eli/etat/leg/loi/1991/07/27/n1/consolide/20220821#art_28septies. [134]

Government of Luxembourg (1983), *Loi du 15 mars 1983 sur les armes et munitions*, https://legilux.public.lu/eli/etat/leg/loi/1983/03/15/n2/jo. [377]

Government of Luxembourg (1879), *Code pénal*, https://legilux.public.lu/eli/etat/leg/code/penal/20240308#art_383. [189]

Government of Luxembourg (1803), *Code Civile*, https://legilux.public.lu/eli/etat/leg/code/civil/20240801. [135]

Government of Mexico (2024), *Código Civil Federal*, https://mexico.justia.com/federales/codigos/codigo-civil-federal/#:~:text=El%20C%C3%B3digo%20Civil%20Federal%20es,patria%20potestad%20y%20a%20la%20adopci%C3%B3n. [265]

Government of Mexico (2010), *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, https://www.gob.mx/indesol/documentos/ley-federal-de-proteccion-de-datos-personales-en-posesion-de-los-particulares. [263]

Government of Mexico (2008), *Ley General Para El Control Del Tabaco*, https://www.gob.mx/cms/uploads/attachment/file/129568/Ley_General_para_el_Control_del_Tabaco.pdf. [339]

Government of Mexico (1984), *Ley General de Salud*, https://dof.gob.mx/nota_detalle.php?codigo=4652777&fecha=07/02/1984#gsc.tab=0. [310]

Government of Mexico (1972), *Ley Federal De Armas De Fuego Y Explosivos*, https://www.diputados.gob.mx/LeyesBiblio/pdf/LFAFE.pdf. [378]

Government of Mexico (1931), *Código Penal Federal*, https://www.oas.org/dil/esp/C%C3%B3digo%20Penal%20Federal%20Mexico.pdf. [190]

Government of Mexico (1928), *Codigo Civil*, https://www.dof.gob.mx/nota_to_imagen_fs.php?codnota=4590686&fecha=26/05/1928&cod_diario=196957. [264]

Government of New Zealand (2020), *Privacy Act*, https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html. [269]

Government of New Zealand (2013), *Sale and Supply of Alcohol Regulations*, https://www.legislation.govt.nz/regulation/public/2013/0459/latest/DLM5736981.html?search=sw_096be8ed81dc32cb_documents_25_se&p=1&sr=1. [313]

Government of New Zealand (2012), *Sale and Supply of Alcohol Act*, https://www.legislation.govt.nz/act/public/2012/0120/latest/DLM3339341.html?search=sw_096be8ed81e794a9_approved_25_se&p=1&sr=0. [312]

Government of New Zealand (2010), *Regulatory Impact Statement: Reducing knife crimes*, https://www.justice.govt.nz/assets/Regulatory-Impact-Statement-Reducing-Knife-Crime.pdf. [382]

Government of New Zealand (1993), *Films, Videos, and Publications Classifications Act*, https://www.legislation.govt.nz/act/public/1993/0094/latest/DLM312895.html. [191]

© OECD 2025

Government of New Zealand (1990), *Smokefree Environments and Regulated Products Act*, https://www.legislation.govt.nz/act/public/1990/0108/latest/whole.html#LMS428474. [341]

Government of New Zealand (1981), *Summary Offences Act*, https://www.legislation.govt.nz/act/public/1981/0113/latest/whole.html#DLM53545. [380]

Government of New Zealand (1961), *Crimes Act*, https://www.legislation.govt.nz/act/public/1961/0043/latest/whole.html#DLM329710. [381]

Government of Norway (2021), *Lov om våpen, skytevåpen, våpendelar og ammunisjon*, https://lovdata.no/dokument/NL/lov/2018-04-20-7/KAPITTEL_3#%C2%A710. [383]

Government of Norway (2018), *Personopplysningsloven*, https://lovdata.no/dokument/NL/lov/2018-06-15-38. [271]

Government of Norway (2017), *Tobakkssalgsforskriften*, https://lovdata.no/dokument/LTI/forskrift/2017-09-21-1446. [342]

Government of Norway (2015), *Lov om beskyttelse av mindreårige mot skadelige bildeprogram mv*, https://lovdata.no/dokument/NL/lov/2015-02-06-7. [137]

Government of Norway (1990), *Alkoholloven – alkhl*, https://lovdata.no/dokument/NL/lov/1989-06-02-27#:~:text=Kort%20om%20loven&text=Alkoholloven%20er%20en%20norsk%20lov,generelle%20forbruket%20av%20alkoholholdige%20drikkevarer. [314]

Government of Poland (2018), *Ustawa z 10 maja 2018 o ochronie danych osobowych*, https://uodo.gov.pl/pl/395/1192. [272]

Government of Poland (1999), *Ustawa Z Dnia 21 Maja 1999 R. O Broni I Amunicji*, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19990530549/U/D19990549Lj.pdf. [384]

Government of Poland (1995), *Ustawa z dnia 9 listopada 1995 r.o ochronie zdrowia przed następstwami używania tytoniu i wyrobów*, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19960100055/U/D19960055Lj.pdf. [343]

Government of Poland (1992), *Ustawa o radiofonii i telewizji*, https://lexlege.pl/ustawa-o-radiofonii-i-telewizji/rozdzial-6b-platformy-udostepniania-wideo/14976/. [138]

Government of Poland (1982), *Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi*, https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19820350230. [315]

Government of Poland (1964), *Kodeks cywilny*, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19640160093/U/D19640093Lj.pdf. [192]

Government of Portugal (2019), *Lei n.º 58/2019, de 08 de Agosto Lei de Proteção de Dados Pessoais*, https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=3118&tabela=leis&nversao=. [273]

Government of Portugal (2017), *Lei n.º 63/2017*, https://files.diariodarepublica.pt/1s/2017/08/14900/0445504477.pdf. [344]

Government of Portugal (2013), *Decreto-Lei.º 50/2013, de 16 de abril*, https://diariodarepublica.pt/dr/detalhe/decreto-lei/50-2013-260432. [316]

© OECD 2025

Government of Portugal (2007), *Lei da Televisão e dos Serviços Audiovisuais a Pedido*, https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=923&tabela=leis. [139]

Government of Portugal (2006), *Regime jurídico das armas e suas munições*, https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2006-34574575. [385]

Government of Portugal (1966), *Código Civil*, https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1966-34509075. [193]

Government of Slovenia (2022), *2305. Splošni akt o zaščiti otrok v avdiovizualnih medijskih storitvah, stran 7000*, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2022-01-2305?sop=2022-01-2305. [142]

Government of Slovenia (2022), *Zakon o varstvu osebnih podatkov (ZVOP-2)*, https://pisrs.si/pregledPredpisa?id=ZAKO7959. [275]

Government of Slovenia (2017), *Zakon o omejevanju uporabe tobačnih izdelkov*, https://pisrs.si/pregledPredpisa?id=ZAKO6717. [346]

Government of Slovenia (2011), *Zakon o avdiovizualnih medijskih storitvah (ZAvMS)*, https://pisrs.si/pregledPredpisa?id=ZAKO6225. [141]

Government of Slovenia (2003), *Zakona o omejevanju porabe alkohola*, https://pisrs.si/pregledPredpisa?id=ZAKO3130. [318]

Government of Slovenia (2001), *Zakon o orožju*, https://pisrs.si/pregledPredpisa?id=ZAKO1440. [387]

Government of Spain (2025), *Anteproyecto de ley orgánica para la protección de las personas menores de edad en los entornos digitales: Memoria del análisis de impacto normativo*, https://www.mpr.gob.es/servicios/participacion/audienciapublica/Documents/VSGT%202024/2024-0921%20APLO%20menores%20entornos%20digitales/MAIN.pdf. [395]

Government of Spain (2024), *El Gobierno aprueba el Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales*, https://www.mpr.gob.es/prencom/notas/Paginas/2024/04062024-proteccion-menores-entorno-digital.aspx. [145]

Government of Spain (2022), *Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual*, https://www.boe.es/buscar/act.php?id=BOE-A-2022-11311. [143]

Government of Spain (2018), *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*, https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673. [276]

Government of Spain (2006), *Ley 28/2005, de 26 de diciembre, de medidas sanitarias frente al tabaquismo y reguladora de la venta, el suministro, el consumo y la publicidad de los productos del tabaco*, https://www.boe.es/buscar/act.php?id=BOE-A-2005-21261. [347]

Government of Spain (1993), *Real Decreto 137/1993, de 29 de enero, por el que se aprueba el Reglamento de Armas*, https://www.boe.es/buscar/act.php?id=BOE-A-1993-6202. [388]

Government of Spain (1992), *Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana*, https://www.boe.es/buscar/act.php?id=BOE-A-1992-4252. [319]

Government of Spain (1889), *Código Civil*, [144]

© OECD 2025

https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/InstListDownload/Codigo_Civil.PDF.

Government of Sweden (2018), *Dataskyddslagen (Lag 2018:218)*, https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218/. [277]

Government of Sweden (2018), *Lag (2018:2088) om tobak och liknande produkter*, https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-20182088-om-tobak-och-liknande-produkter_sfs-2018-2088/. [348]

Government of Sweden (2010), *Alkohollag*, https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/alkohollag-20101622_sfs-2010-1622/. [320]

Government of Sweden (2010), *Radio and Television Act*, https://mediemyndigheten.se/globalassets/om-mediemyndigheten/mediemyndighetens-verksamhet/dokument/radio-och-tv-lag/the-swedish-radio-and-television-act.pdf. [147]

Government of Sweden (1988), *Förbud beträffande knivar och andra farliga föremål*, https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-1988254-om-forbud-betraffande-knivar-och_sfs-1988-254/. [389]

Government of Switzerland (2024), *Loi fédérale sur les produits du tabac et les cigarettes électroniques*, https://www.fedlex.admin.ch/eli/cc/2024/457/fr. [349]

Government of Switzerland (2022), *Loi fédérale sur la protection des mineurs dans les secteurs du film et du jeu vidéo*, https://www.fedlex.admin.ch/eli/oc/2024/331/fr. [149]

Government of Switzerland (2020), *Federal Act on Data Protection*, https://www.fedlex.admin.ch/eli/cc/2022/491/en. [278]

Government of Switzerland (1997), *Loi fédérale sur les armes, accessoires d'armes et munitions*, https://www.fedlex.admin.ch/eli/cc/1998/2535_2535_2535/en. [390]

Government of Switzerland (1937), *Criminal Code*, https://www.fedlex.admin.ch/eli/cc/54/757_781_799/en. [194]

Government of Switzerland (1932), *Alkoholgesetz, AlkG*, https://www.fedlex.admin.ch/eli/cc/48/425_437_457/de#a57. [321]

Government of Switzerland (1907), *Civil Code*, https://www.fedlex.admin.ch/eli/cc/24/233_245_233/en. [279]

Government of Switzerland (1907), *Code civil suisse du 10 décembre 1907*, https://www.fedlex.admin.ch/eli/cc/24/233_245_233/fr. [150]

Government of the Netherlands (2021), *Alcoholwet*, https://wetten.overheid.nl/BWBR0002458/2021-07-01. [311]

Government of the Netherlands (2021), *code voor kinderrecthten*, https://codevoorkinderrechten.nl/wp-content/uploads/2022/02/Code-voor-Kinderrechten-EN.pdf. [268]

Government of the Netherlands (2018), *Uitvoeringswet Algemene verordening gegevensbescherming*, https://wetten.overheid.nl/BWBR0040940/2018-05-25. [267]

© OECD 2025

Government of the Netherlands (2017), *Wet wapens en munitie*, https://wetten.overheid.nl/BWBR0008804/2017-09-01. [379]

Government of the Netherlands (2008), *Mediawet*, https://www.cvdm.nl/voor-mediamakers/regelgeving/mediawet/. [136]

Government of the Netherlands (1990), *Tabaks- en rookwarenwet*, https://wetten.overheid.nl/BWBR0004302/2024-07-01#Paragraaf2. [340]

Government of the Slovak Rebublic (2022), *Zákon o mediálnych službách*, https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2022/264/20230101#paragraf-62.odsek-1. [140]

Government of the Slovak Republic (2018), *Zakon z 29. novembra 2017 o ochrane osobných údajov a o zmene a doplnení niektorých zákonov*, https://www.slov-lex.sk/static/pdf/2018/18/ZZ_2018_18_20240701.pdf. [274]

Government of the Slovak Republic (2004), *ZÁKON z 26. Mája 2004 o ochrane nefajčiarov a o zmene doplnení niektorých zákonov*, https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2004/377/. [345]

Government of the Slovak Republic (2003), *Zákon č. 190/2003 Z. z. Zákon o strelných zbraniach a strelive a o zmene a doplnení niektorých zákonov*, https://www.zakonypreludi.sk/zz/2003-190. [386]

Government of the Slovak Republic (1996), *Zákon č. 219/1996 Z. z. Zákon Národnej rady Slovenskej republiky o ochrane pred zneužívaním alkoholických nápojov a o zriaďovaní a prevádzke protialkoholických záchytných izieb*, https://www.zakonypreludi.sk/zz/1996-219. [317]

Government of the United Kingdom (2025), *'Ronan's Law' to see toughest crackdown yet on knife sales online*, https://www.gov.uk/government/news/ronans-law-to-see-toughest-crackdown-yet-on-knife-sales-online?fbclid=IwY2xjawIim81leHRuA2FlbQIxMQABHeJvfkkZQReH-NN62t6uJ7fiGm-ihC3mF5QGYjuzucnrrBsKoXq0OVz5Ew_aem_-OuU82FNQCssqG1e0S3Ojg. [53]

Government of the United Kingdom (2024), *Sale of knives: voluntary agreement by retailers*, https://www.gov.uk/government/publications/sale-of-knives-voluntary-agreement-by-retailers/sale-of-knives-voluntary-agreement-by-retailers. [393]

Government of the United Kingdom (2023), *Online Safety Act*, https://www.legislation.gov.uk/ukpga/2023/50. [18]

Government of the United Kingdom (2020), *UK GDPR - Regulation (EU) 2016/679 of the European Parliament and of the Council*, https://www.legislation.gov.uk/eur/2016/679/contents. [284]

Government of the United Kingdom (2018), *Data Protection Act*, https://www.legislation.gov.uk/ukpga/2018/12/contents. [283]

Government of the United Kingdom (2016), *The Tobacco and Related Products Regulations*, https://www.legislation.gov.uk/uksi/2016/507. [351]

Government of the United Kingdom (1988), *Criminal Justice Act*, https://www.legislation.gov.uk/ukpga/1988/33/data.pdf. [392]

Government of the United States (2010), *Title 21, Food and Drugs, cigarettes, smokeless* [355]

© OECD 2025

tobacco, and covered tobacco products, https://www.ecfr.gov/current/title-21/chapter-I/subchapter-K/part-1140.

Government of the United States (1998), *Child Online Privacy Protection Act*, https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa. [287]

Government of the United States (1948), *U.S. Code: Title 18*, https://uscode.house.gov/browse/prelim@title18/part1/chapter71&edition=prelim. [198]

Government of Türkiye (2016), *KİŞİSEL VERİLERİN KORUNMASI KANUNU*, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5. [280]

Government of Türkiye (2007), *Law No. 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed through Such Publications*, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf. [196]

Government of Türkiye (2004), *Türk Ceza Kanunu*, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5237&MevzuatTur=1&MevzuatTertip=5. [195]

Government of Türkiye (2001), *Türk Medenî Kanunu*, https://www.mevzuat.gov.tr/mevzuatmetin/1.5.4721.pdf. [281]

Government of Türkiye (1996), *Tütün Ürünlerinin Zararlarinin Önlenmesi Ve Kontrolü*, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.4207.pdf. [350]

Government of Türkiye (1991), *Ateşli Silahlar, Bıçaklar ve Diğer Aletlere İlişkin Yönetmelik*, http://eng.umut.org.tr/regulation-regarding-firearms-knives-and-other-tools/. [391]

Government of Türkiye (1942), *İspirto Ve İspirtolu İçkiler İnhisari Kanunu*, https://www.mevzuat.gov.tr/MevzuatMetin/1.3.4250.pdf. [322]

Heat Initiative (2024), *Rotten Ratings: 24 Hour's in Apple's App Store*, https://heatinitiative.org/wp-content/uploads/2024/12/Apple-App-Store-Report-18-dec-12_09.pdf. [76]

Heise Online (2025), *Ministry of Family Affairs develops "data-saving age verification"*, https://www.heise.de/en/news/Ministry-of-Family-Affairs-develops-data-saving-age-verification-10318701.html. [114]

IARC (2025), *How IARC works*, https://www.globalratings.com/how-iarc-works.aspx. [70]

IARC (2024), *About IARC*, https://www.globalratings.com/about.aspx. [66]

Idaho State Legislature (2024), *Liability for Publishers and Distributors of Material Harmful to Minors (HB 498)*, https://legislature.idaho.gov/sessioninfo/2024/legislation/h0498/. [203]

Indiana State Legisature (2020), *Motor Vehicles Code*, https://iga.in.gov/laws/2023/ic/titles/9#9-13-2-103.4. [206]

Indiana State Legislature (2024), *Age verification for material harmful to minors (SB 17)*, https://iga.in.gov/legislative/2024/bills/senate/17/details. [204]

Indiana State Legislature (1983), *Criminal Law and Procedure Code*, https://iga.in.gov/laws/2023/ic/titles/35#35-49. [205]

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales [266]

© OECD 2025

(2020), *Code of Good Practice to Guide the Online Processing of Personal Data of Children and Adolescents*, https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/codigobuenaspracticasnna.pdf.

International Age Assurance Working Group (2024), *Joint statement on a common international approach to age assurance*, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/joint-statement-on-a-common-international-approach-to-age-assurance/. [29]

Ireland Data Protection Commission (2021), *Fundamentals for a Child-Oriented Approach to Data Processing*, https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf. [250]

Kansas State Legislature (2024), *Senate Bill 394*, https://www.kslegislature.gov/li/b2023_24/measures/sb394/. [207]

Kansas State Legislature (2011), *Crimes Against the Public Morals*, https://kslegislature.gov/li_2012/b2011_12/statute/021_000_0000_chapter/021_064_0000_article/021_064_0002_section/021_064_0002_k/. [208]

Kentucky State Legislature (2024), *An Act relating to the protection of children (HB 278)*, https://apps.legislature.ky.gov/record/24rs/hb278.html. [209]

Kommission für Jugendmedienschutz (2024), *Unzulässige Inhalte*, https://www.kjm-online.de/themen/technischer-jugendmedienschutz/unzulaessige-inhalte/ (accessed on October 2024). [41]

Korea Personal Information Protection Commission (2022), *Online Personal Information Protection for Children and Adolescents, Principles and Standards*, https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=8159. [259]

KVKK (2020), *Çocukların Kişisel Verilerinin Korunması Bakımından Dikkat Edilmesi Gerekenler*, https://www.kvkk.gov.tr/Icerik/6737/Cocuklarin-Kisisel-Verilerinin-Korunmasi-Bakimindan-Dikkat-Edilmesi-Gerekenler. [282]

La Moncloa (2025), *The Government strengthens the protection of minors in digital environments*, https://www.lamoncloa.gob.es/consejodeministros/resumenes/paginas/2025/250325-rueda-de-prensa-ministros.aspx. [146]

Lexis Nexis Insights (2025), *More Kids' Online Safety Measures Expected in 2025*, https://www.lexisnexis.com/community/insights/legal/capitol-journal/b/state-net/posts/more-social-media-bills-coming-this-year?srsltid=AfmBOoqrEi07QZYiQ-j0lDE_5hdcHSaIuKPCMWTJembwFo0Y-XRVDKvi. [15]

Louisiana State Legislature (2024), *Secure Online Child Interaction and Age Limitation Act*, https://legiscan.com/LA/text/SB162/2023. [166]

Louisiana State Legislature (2023), *Act no. 216 (Provides for attorney general investigation for publishers and distributors of material harmful to minors)*, https://legiscan.com/LA/text/HB77/id/2826932. [211]

© OECD 2025

Lousiana State Legislature (2023), *Liability for publishers and distributors of material harmful to minors (Act No. 440)*, https://legiscan.com/LA/bill/HB142/2022. [210]

migrationsverket (2024), *Your rights as a child in Sweden*, https://www.migrationsverket.se/Privatpersoner/Skydd-och-asyl-i-Sverige/Resettlement/Resettlement-english/Resettlement/For-children-and-teenagers/Your-rights-as-a-child-in-Sweden.html#:~:text=In%20Sweden%2C%20you%20are%20considered,is%20the%20law%20in%20S. [148]

Mississippi State Legislature (2023), *Senate Bill 2346*, https://billstatus.ls.state.ms.us/2023/pdf/history/SB/SB2346.xml. [212]

Montana State Legislature (2024), *Senate Bill 544*, https://leg.mt.gov/bills/2023/billhtml/SB0544.htm. [213]

Nebraska State Legislature (2024), *Online Age Verification Liability Act (LB 1092)*, https://legiscan.com/NE/bill/LB1092/2023. [214]

New York State Legislature (2024), *Stop Addictive Feeds Exploitation (SAFE) for Kids Act (S7694A)*, https://www.nysenate.gov/legislation/bills/2023/S7694/amendment/A#:~:text=2023%2DS7694%20%2D%20Summary,platforms%3B%20establishes%20remedies%20and%20penalties. [167]

New Zealand Privacy Commissioner (2013), *How does the Privacy Act deal with children and teenagers?*, https://privacy.org.nz/tools/knowledge-base/view/2. [270]

NIST (2025), *A.10 IAL2 Remote Identity Proofing*, https://pages.nist.gov/800-63-3-Implementation-Resources/63A/ial2remote/. [52]

North Carolina State Legislature (2023), *Pornography Age Verification Enforcement (PAVE) Act (HB 8)*, https://legiscan.com/NC/text/H8/2023. [215]

North Carolina State Legislature (2023), *General Statute (Chapter 14: Criminal Law)*, https://casetext.com/statute/general-statutes-of-north-carolina/chapter-14-criminal-law/subchapter-vll-offenses-against-public-morality-and-decency/article-26-offenses-against-public-morality-and-decency/section-14-19013-effective-1212024-definitions-for-. [216]

Northern Ireland Statutory Rules (2008), *The Children and Young Persons (Sale of Tobacco etc.) Regulations (Northern Ireland)*, https://www.legislation.gov.uk/nisr/2008/306/contents/made. [354]

NSW Government (2007), *Liquor Act*, https://legislation.nsw.gov.au/view/html/inforce/current/act-2007-090. [400]

OECD (2025), *Age assurance online for children's safety and well-being: A benchmarking of age assurance policies and practices among 50 online services used by children*, https://doi.org/10.1787/a19853ab-en. [10]

OECD (2024), *OECD Digital Economy Outlook 2024 (Volume 1): Embracing the Technology Frontier*, OECD Publishing, Paris, https://doi.org/10.1787/a1689dc5-en. [4]

OECD (2024), "Towards digital safety by design for children", *OECD Digital Economy Papers*, No. 363, OECD Publishing, Paris, https://doi.org/10.1787/c167b650-en. [5]

OECD (2023), *Expert Roundtable on Digital Safety by Design for Children: Summary of Key* [6]

© OECD 2025

Points (Internal Document), https://one.oecd.org/document/DSTI/CDEP(2023)28/en/pdf.

OECD (2023), "Transparency reporting on child sexual exploitation and abuse online", *OECD Digital Economy Papers*, No. 357, OECD Publishing, Paris, https://doi.org/10.1787/554ad91f-en. [3]

OECD (2022), "Putting people first in digital transformation: Background paper for the CDEP Ministerial meeting", *OECD Digital Economy Papers*, No. 339, OECD Publishing, Paris, https://doi.org/10.1787/865f8426-en. [1]

OECD (2021), "Children in the digital environment: Revised typology of risks", *OECD Digital Economy Papers*, No. 302, OECD Publishing, Paris, https://doi.org/10.1787/9b8f222e-en. [2]

OECD (2021), *Guidelines for Digital Service Providers*, https://legalinstruments.oecd.org/api/download/?uri=/private/temp/cecf7c1a-2590-4aaf-98d7-2a5f74290b92.pdf&name=Guidelines%20for%20Digital%20Service%20Providers.pdf. [12]

OECD (2021), *Recommendation of the Council on Children in the Digital Environment*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389. [11]

Ofcom (2025), *Guidance on highly effective age assurance and other part 5 duties*, https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/guidance-on-highly-effective-age-assurance-and-other-part-5-duties.pdf?v=388810. [197]

Ofcom (2025), *Guidance on highly effective age assurance for part 3 services*, https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/part-3-guidance-on-highly-effective-age-assurance.pdf?v=395680. [153]

Ofcom (2025), *Guidance on highly effective age assurance for part 3 services*, https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/part-3-guidance-on-highly-effective-age-assurance.pdf?v=395680. [154]

Ofcom (2025), *Statement: Protecting children from harms online*, https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/statement-protecting-children-from-harms-online. [152]

Ofcom (2024), *Consultation: Protecting children from harms online*, https://www.ofcom.org.uk/online-safety/protecting-children/protecting-children-from-harms-online/. [44]

Ofcom (2024), *New rules for online services: what you need to know*, https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/guide-for-services/#who. [161]

Ofcom (2024), *Repeal of the VSP regime: what you need to know*, https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/repeal-of-the-vsp-regime/. [151]

Ofcom (2023), *Joint statement: Working with other regulators to protect children online*, https://www.ofcom.org.uk/online-safety/protecting-children/age-verification-joint-statement/. [31]

Ofcom (2022), *Children's Online User Ages Quantitative Research Study*, https://www.ofcom.org.uk/__data/assets/pdf_file/0015/245004/children-user-ages-chart- [24]

© OECD 2025

pack.pdf.

Office of the Australian Information Commissioner (2025), *Children's Online Privacy Code*, https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes/childrens-online-privacy-code#section-key-milestones. [78]

Office of the Australian Information Commissioner (2022), *Australian Privacy Principles guidelines, Chapter B: Key Concepts*, https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-b-key-concepts. [228]

Office of the Privacy Commissioner Canada (2021), *Guidelines for obtaining meaningful consent*, https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/. [233]

Office of the Privacy Commissioner Canada (2015), *Collecting from kids? Ten tips for services aimed at children and youth*, https://www.priv.gc.ca/en/privacy-topics/business-privacy/bus_kids/02_05_d_62_tips/#fn7. [232]

Oklahoma State Legislature (2024), *Oklahoma Statutes (Title 21)*, https://casetext.com/statute/oklahoma-statutes/title-21-crimes-and-punishments/chapter-39-oklahoma-law-on-obscenity-and-child-pornography/display-of-materials-harmful-to-minors/section-104075-effective-1112024-definitions. [218]

Oklahoma State Legislature (2024), *Senate Bill 1959*, http://www.oklegislature.gov/BillInfo.aspx?Bill=sb1959&Session=2400. [217]

Online Safety Australia (2025), *Consultation: Phase 2 Codes*, https://onlinesafety.org.au/phase-two-codes/. [39]

Open Rights Group (2023), *UK online safety bill will mandate dangerous age verification for much of the web*, https://www.openrightsgroup.org/publications/uk-online-safety-bill-will-mandate-dangerous-age-verification-for-much-of-the-web/. [8]

Parliament of Australia (2025), *History of censorship and classification in Australia*, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Completed_inquiries/2010-13/classificationboard/report/c02. [59]

Parliament of Scotland (2010), *Tobacco and Primary Medical Services (Scotland) Act*, https://www.legislation.gov.uk/asp/2010/3/contents. [353]

Parliament of Scotland (2005), *Licensing (Scotland) Act*, https://www.legislation.gov.uk/asp/2005/16/section/102. [324]

PEGI (2017), *About us*, https://pegi.info/. [62]

PEGI (2017), *Facebook*, https://pegi.info/search-pegi?q=facebook&op=Search&age%5B%5D=&descriptor%5B%5D=&publisher=&platform%5B%5D=&release_year%5B%5D=&page=1&form_build_id=form-3uJbaNd4EcfukC_7m3cu4CXIyWbNxHmivY6Lo1ANMpk&form_id=pegi_search_form. [397]

PEGI (2017), *How we rate games*, https://pegi.info/page/how-we-rate-games. [65]

PEGI (2017), *Instagram*, https://pegi.info/search-pegi?q=Instagram&op=Search&age%5B%5D=&descriptor%5B%5D=&publisher=&platform%5B%5D=&release_year%5B%5D=&page=1&form_build_id=form- [398]

© OECD 2025

5hC9DSrYmL96S2fJcte37r8EVtugDCKyoE6wj5ZS6nc&form_id=pegi_search_form.

PEGI (2017), *The PEGI Code of Conduct*, https://pegi.info/pegi-code-of-conduct. [74]

Personal Information Protection Commission (2020), *Guidelines for the Act on the Protection of Personal Information (General Rules)*, https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/. [255]

Personal Information Protection Commission (2020), *Q&A regarding "Guidelines on the Act on the Protection of Personal Information"*, https://www.ppc.go.jp/files/pdf/2412_APPI_QA.pdf. [256]

Public Health Law Centre at Mitchell Hamline School of Law (2022), *Online sales of e-cigarettes and other tobacco products*, https://www.publichealthlawcenter.org/sites/default/files/resources/Online-Sales-E-Cigarettes-Other-Tobacco-Products.pdf. [56]

Revealing Reality (2022), *Families'attitudes toward age assurance (Research commissioned by the ICO and Ofcom)*, https://www.ofcom.org.uk/__data/assets/pdf_file/0026/245195/DRCF-Ofcom-ICO-age-assurance.pdf. [9]

Rideout, V. et al. (2022), *Common Sense census: Media use by tweens and teens, 2021.*, https://www.commonsensemedia.org/sites/default/files/research/report/8-18-census-integrated-report-final-web_0.pdf. [23]

Sénat (2023), *LOI n° 2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne*, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047799533/. [159]

Smirnova, S., S. Livingstone and M. Stoilova (2021), *Understanding of user needs and problems: A rapid evidence review of age assurance and parental controls*, https://euconsent.eu/download/understanding-of-user-needs-and-problems-a-rapid-evidence-review-of-age-assurance-and-parental-controls/. [7]

South Carolina State Legislature (2024), *House Bill 3424*, https://www.scstatehouse.gov/sess125_2023-2024/bills/3424.htm. [219]

South Carolina State Legislature (1987), *South Carolina Code of Laws*, https://www.scstatehouse.gov/code/t16c015.php. [220]

South Dakota State Legislature (2025), *An Act to require age verification by websites containing material that is harmful to minors, and to provide a penalty therefor (House Bill 1053)*, https://sdlegislature.gov/Session/Bill/25525/276255. [221]

Tech Policy Press (2023), *144 State Bills Aim to Secure Child Online Safety As Congress Flounders*, https://www.techpolicy.press/144-state-bills-aim-to-secure-child-online-safety-as-congress-flounders/. [13]

Tennessee State Legislature (2024), *Protect Tennessee Minors Act (Senate Bill 1792)*, https://legiscan.com/TN/bill/SB1792/2023. [222]

Tennessee State Legislature (2024), *Protecting Children from Social Media Act (HB 1891)*, https://legiscan.com/TN/text/HB1891/id/2905491. [168]

Texas State Legislature (2023), *Securing Children Online through Parental Empowerment (SCOPE) Act (HB 18)*, [169]

© OECD 2025

https://capitol.texas.gov/BillLookup/History.aspx?LegSess=88R&Bill=HB18.

Texas State Legislature (1993), *Texas Penal Code*, https://statutes.capitol.texas.gov/Docs/PE/htm/PE.43.htm#43.21. [223]

UK Home Office (2014), *Guidance on mandatory licensing conditions*, https://www.gov.uk/government/publications/guidance-on-mandatory-licensing-conditions. [401]

UK Public General Acts (2003), *Licensing Act*, https://www.legislation.gov.uk/ukpga/2003/17/section/146. [323]

UK Statutory Instruments (2007), *The Children and Young Persons (Sale of Tobacco etc.) Order 2007*, https://www.legislation.gov.uk/uksi/2007/767/contents/made. [352]

United Kingdom Information Commissioners Office (2025), *What rights do children have?*, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr/what-rights-do-children-have/. [285]

United Kingdom Information Commissioners Office (2024), *Age assurance for the Children's code*, https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code/. [88]

United Kingdom Information Commissioners Office (2024), *Age assurance for the Children's code*, https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code/. [286]

United Kingdom Information Commissioners Office (2020), *Age appropriate design: a code of practice for online services (the Children's Code)*, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/. [77]

United Kingdom Information Commissioner's Office (2024), *Social media and video sharing platforms put on notice over poor children's privacy practices*, https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/08/social-media-and-video-sharing-platforms-put-on-notice-over-poor-children-s-privacy-practices/. [21]

United Kingdom Parliament (2025), *Data (Use and Access) Bill*, https://bills.parliament.uk/bills/3825. [81]

United Kingdom Parliament (2024), *Government plans to address children vaping*, https://lordslibrary.parliament.uk/government-plans-to-address-children-vaping/. [55]

United States Code of Federal Regulations (2013), *Children's Online Privacy Protection Rule*, https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312. [19]

United States Congress (2024), *Bill - Kids Online Safety and Privacy Act*, https://www.congress.gov/bill/118th-congress/senate-bill/2073/text#toc-id43fe8c4d-e881-41b0-819c-a88c54ed5043. [155]

United States Congress (2020), *S.1253 - Preventing Online Sales of E-Cigarettes to Children Act*, https://www.congress.gov/bill/116th-congress/senate-bill/1253. [54]

United States District Court (2024), *Free Speech Coalition & ors. v. Ken Paxton*, https://www.ca5.uscourts.gov/opinions/pub/23/23-50627-CV0.pdf. [396]

© OECD 2025

United States District Court (2024), *NetChoice, LLC v. Reyes*, https://casetext.com/case/netchoice-llc-v-reyes. [173]

United States Federal Trade Commission (2022), *Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges*, https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations. [20]

United States Public Health Service (2023), *Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory*, https://www.hhs.gov/surgeongeneral/priorities/youth-mental-health/social-media/index.html. [22]

United States Supreme Court (2025), *Free Speech Coalition, Inc., et al., Petitioners v. Ken Paxton, Attorney General of Texas*, https://www.supremecourt.gov/search.aspx?filename=/docket/docketfiles/html/public/23-1122.html. [170]

USK (2025), *Age classification for games and apps*, https://usk.de/en/home/age-classification-for-games-and-apps/. [68]

Utah State Legislature (2024), *Social Media Amendments (HB 464)*, https://le.utah.gov/~2024/bills/static/HB0464.html. [171]

Utah State Legislature (2024), *Social Media Regulation Amendments (SB 194)*, https://le.utah.gov/~2024/bills/static/SB0194.html. [172]

Utah State Legislature (2023), *Online Pornography Viewing Age Requirements (S.B. 287)*, https://le.utah.gov/~2023/bills/static/SB0287.html. [224]

Virginia State Legislature (2023), *Senate Bill 1515*, https://lis.virginia.gov/cgi-bin/legp604.exe?231+sum+SB1515. [225]

WeProtect Global Alliance (2025), *Who we are*, https://www.weprotect.org/about-us/who-we-are/. [399]

Wyoming State Legislature (2025), *House Bill 0043 - Age verification for websites with harmful material*, https://www.wyoleg.gov/Legislation/2025/HB0043. [226]

© OECD 2025

Notes

[1] OECD research usually focusses only on national initiatives, but this paper examines a number of laws that have been enacted by individual states within the United States. It does so because global companies operating in these jurisdictions need to apply these laws, making them relevant to the overall age assurance landscape. The United States is the only OECD Member country where a trend of sub-national jurisdictions enacting laws mandating age assurance is observed. The laws analysed are only those governing access to pornography and social media.

[2] The OECD Recommendation on Children in the Digital Environment defines children as individuals below the age of eighteen years, recognising that different age thresholds may be appropriate in providing certain legal protections (OECD, 2021[11]).

[3] Throughout this paper, where "parent" is used it should be read to cover also carers and guardians.

[4] The OECD Recommendation on Children in the Digital Environment defines digital service providers as "any natural or legal person that provides products and services, electronically and at a distance" (OECD, 2021[11]).

[5] An implied legal requirement must be inferred from the context in which it appears, but that does not mean it has any less force than an express requirement. An express legal requirement is not stronger or more enforceable than an implied one – it is just overtly stated whereas an implied one is not.

[6] For instance, Japan's Act on Establishment of Enhanced Environment for Youth's Safe and Secure Internet Use (Government of Japan, 2008[127]) prescribes device level filtering as a means of protecting children online.

[7] An independent organisation the WeProtect Global Alliance brings together over 300 members from governments, the private sector, civil society and intergovernmental organisations to develop policies and solutions to protect children from sexual exploitation and abuse online (WeProtect Global Alliance, 2025[399]).

[8] The Centre for Information Policy Leadership is "a global privacy and data policy think and do tank (that) works with industry leaders, regulatory authorities and policymakers to develop global solutions and best practices for privacy and responsible use of data" (Centre for Information Policy Leadership, 2024[394])

[9] Many existing company practices setting age limits on these services arise from those limits set in data protection and privacy laws. These laws are set out in section 5.

[10] Noting that France also has specific laws dealing explicitly with certain content under its criminal law regime and aimed at online games, and Switzerland's law partially transposes the AVMSD.

© OECD 2025

[11] For instance, a 2023 study found that of the OECD countries from the EU listed in Table 3.1, seven (Belgium, Czechia, Germany, Greece, Italy, Lithuania and Slovenia) had no VSP under their jurisdiction (European Audiovisual Observatory[36]).

[12] Texas has a second law directly covering access to pornography and requiring age assurance for this purpose. While currently in force (after having been left operational by United States District Court (United States District Court, 2024[396])), the law is (as of March 2025) pending a Supreme Court challenge, and oral arguments were heard in early 2025 (United States Supreme Court, 2025[170]). Accordingly, given its uncertain status, it is not included in this report.

[13] Sites are those established in France or outside the European Union, as well as those located in the European Union provided that they appear on a ministerial decree (Arcom, 2025[50]).

[14] See for example s114 of the Liquor Act 2007 (NSW) in Australia (NSW Government, 2007[400]).

[15] See for example the United Kingdom's Home Office Guidance on Mandatory Licensing Conditions (UK Home Office, 2014[401]).

[16] See for example the European Union's Tobacco Products Directive (European Union, 2014[402]).

[17] It is noted that as a number of OECD countries deal with this issue on a decentralised basis, this section does not provide a comprehensive analysis of all laws covering the sale of alcohol, knives and cigarettes but rather considers only those countries which have one law on the issue.

[18] In 1997, the ESRB established an Online Rating Notice to warn consumers of user-generated content in online-enabled games and on websites (ESRB, 2025[61]).

[19] As of March 2025, these are Epic Games, Fortnite, Google Play, Luna, Meta Quest, Microsoft, Nintendo eShop, One Store, Pico and Playstation Store (IARC, 2024[66]).

[20] See for instance PEGI's guidance on Facebook (PEGI, 2017[397])and Instagram (PEGI, 2017[398])

[21] Despite leaving the European Union, the United Kingdom's data protection regime remains in line with GDPR by virtue of the Data Protection Act (the UK GDPR) (Government of the United Kingdom, 2018[283]).

[22] It is noted that the GDPR requirements apply only to those which meet the definition of an "information society service". See the relevant field in Annex D for that definition.

[23] This is the situation under PIPEDA (Government of Canada, 2000[231]), but in Canada some sub-national laws may set a different minimum age.

[24] One of these countries, however (Spain), is in the process of reviewing the appropriateness of that age (Government of Spain, 2025[395]).

© OECD 2025