

Draft name Draft of an Act on the Protection of Minors from Access to Pornographic Content on the Internet Lead ministry and cooperating ministries Ministry of Digital Affairs Person responsible for the draft: Minister, Secretary of State or Undersecretary of State Michał Gramatyka, Secretary of State at the Ministry of Digital Affairs Contact details for the draft supervisor Marzena Sawicka, Director of the Telecommunications Department at the Ministry of Digital Affairs, Marzena.Sawicka@cyfra.gov.pl +48 22 245 59 18	Drawn up on 02.06.2026 Source: Own initiative Number in the List of Legislative and Programming Works of the Council of Ministers: UD179
--	---

REGULATORY IMPACT ASSESSMENT

1. What issue is being addressed?

Children and young people in Poland have far too easy access to content that is widely regarded as harmful. In particular, it is far too easy to access pornography online. A number of studies carried out in Poland show that this is a major problem, particularly amongst boys. According to research, as many as 73.0% of children and 71.1% of young people report that it is very easy to access pornographic content online ⁽¹⁾.

Among the factors that facilitate minors' access to pornographic content we should particularly mention the increasing number of children who have their own smartphone with unlimited access to the Internet. This means that young people have access to all online content, including pornographic content, at any time and anywhere. Where no parental control arrangements have been put in place, adult guardians are not aware of what content their children are watching, nor are they able to control what their children are doing online on an ongoing basis. Websites containing pornographic content are not effectively protected against access by minors. At present, providers of pornographic websites do not have any effective safeguards in place to prevent access by minors. Once on the website, it is sufficient to tick a box stating that the visitor is at least 18 years old. Once the visitor has done this, access to any free pornographic content is obtained.

What's more, pornographic content in particular ranks highly in search results, which is why it is very easy to find. This translates directly into a high risk of accidental contact with this type of content, even if the minor does not directly search for it.

What is particularly worrying is the average age at which children are first exposed to pornographic content, which averages just under 11 years old, whilst among older teenagers it is 12 years old. Almost one in five (18.5%) of those surveyed were under 10 years old when they first came into contact with sexual content. Pornographic content is found twice as often by children whose parents have not set rules for internet use. This means that only the parents of one in two children talk to their child about the websites they visit online. Research also suggests that young people most often come into contact with pornographic content via their mobile phones. At the same time, as many as 80% of children say they do not have any parental control software installed on their devices⁽²⁾. In view of the above, access to harmful content – obtained mainly via the internet – should be regarded as one of the factors posing the greatest threat to children's health and psychophysical development. This is an issue that has been the subject of numerous analyses and studies, and one that requires an appropriate and immediate response. It should be emphasised, however, that in the case of certain other harmful content available outside the internet – for example, presented in television programmes – this matter is governed by separate legislation which is already in force. In the case of games, on the other hand, child protection is based on the self-regulatory classification system PEGI (Pan European Game Information) – the European rating system for computer games.

Report by the Scientific and Academic Computer Network – National Research Institute, hereinafter referred to as 'NASK-PIB', 'Nastolatki 3.0 Raport z ogólnopolskiego badania uczniów'⁽³⁾ from 2023 indicates that over half of teenagers (53.7%) say that their parents do not set any rules regarding internet use in terms of time spent online and access to content. At the same time, nearly one in four young internet users believe that the controls imposed by their parents on their internet usage time (28.8%) and access to online content (28.9%) are ineffective.

⁽¹⁾ Nastolatki wobec pornografii cyfrowej. Trajektorie użytkowania. Raport z badań ogólnopolskich. NASK-PIB 2022, <https://www.nask.pl/pl/raporty/raporty/5077,Raport-Nastolatki-wobec-pornografii-cyfrowej.html>, [accessed 16 March 2026].

⁽²⁾ Ibid.

⁽³⁾ NASK-PIB research report 'Nastolatki 3.0 Raport z ogólnopolskiego badania uczniów' from 2023 – <https://www.nask.pl/pl/raporty/raporty/5315,Raport-quotNastolatki-30quot.html> [accessed 16 March 2026]

Children and young people are at a crucial stage in the development of their identity, their value system and their ability to distinguish between right and wrong. During this period, they are particularly vulnerable to external influences, including those from the Internet. Pornographic content, often marked by violence, can disrupt this process. Exposure to such material can cause a wide range of problematic reactions in children, including desensitisation to violence, increased aggression, sleep problems, anxiety and difficulty managing their emotions. Minors lack the cognitive tools to critically analyse what they see, which may lead them to perceive such behaviour – even subconsciously – as the norm or a role model. Access to pornographic content can lead to addiction, difficulties concentrating, a reduced motivation to study, and problems in developing healthy relationships with peers. Prolonged exposure to content that promotes negative role models leads to low self-esteem, depression and social withdrawal in children.

This means that children whose parents do not use parental control tools have free and unrestricted access to all content, including pornographic content, like adults. It is worth noting, however, that even if a parent installs such a tool, it will not fully protect their child from pornographic content, as it is enough for just one person in a peer group to have access to such content and share it with other children. Therefore, the only effective barrier to protect minors is the use of blocking measures by providers of pornographic content.

According to the assessment set out in the document ‘Negatywne konsekwencje korzystania z pornografii’⁽⁴⁾, the scale of the issue has long since grown to such an extent that pornography, due to its easy accessibility to children and young people, must be recognised as a serious public health problem. Pornographic content, most of which is available free of charge on the internet, is cited as one of the main factors contributing to the psychological and physical destabilisation of minors. It should also be noted that for many minors, pornography remains one of the sources of information about human sexuality; combined with a lack of adequate supervision of children’s internet use, this may result in a distorted perception of sexuality and gender roles during adolescence and the entrenchment of potentially pathological views upon reaching adulthood.

The European Commission, in its Communication ‘A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+)’⁽⁵⁾, also notes that age-inappropriate content is easily accessible. Children admit that they view pornography at a young age, which influences their perceptions of what a healthy relationship looks like.

These studies highlight the growing problem of minors having too easy access to pornographic content and the lack of, or insufficient effectiveness of, mechanisms to restrict access to such content. The proposed legislation is intended to address these issues; as outlined below, it provides for the imposition of new obligations on providers of electronic services, in particular on providers of websites (where pornographic content available to minors is or could potentially be presented).

Despite the growing availability of parental control tools and the educational and awareness-raising campaigns being run in this field – both by public authorities and representatives of telecoms operators – their actual use by parents and legal guardians remains at an alarmingly low level. According to reports prepared by NASK-PIB, only around 28% of parents declare active use of software that filters or restricts access to harmful content online, and only 13% of children confirm that such software is used. Parents cite a lack of sufficient knowledge about the technical solutions available, a lack of the skills to use them, or their ineffectiveness as reasons for not using such solutions. In Poland, parental control applications are downloaded by a relatively small percentage of people compared to the number of households. Such a low level of technical safeguards justifies the need to introduce the additional preventative obligations provided for in the proposed law.

The pornographic content covered by the draft bill is not illegal and is available to adult audiences. However, given that children’s emotional maturity, critical thinking skills and knowledge of the world are still developing, and in view of the negative impact such content may have on their emotional, cognitive and social development, it is essential to introduce mechanisms to restrict minors’ access to pornographic content. Given the negative impact of the content on the emotional, cognitive and social development of children and young people, legislative action is necessary.

2. The recommended solution, including planned intervention tools and expected impact

The most effective way of preventing minors from accessing pornographic content is undoubtedly a multi-pronged approach, i.e. running educational campaigns, providing parental control tools and taking legislative action, all at the same time. Currently, both public administration bodies and non-governmental organizations carry out a number of educational and information activities addressed to minors, as well as their parents and teachers. There are also parental control tools and applications (both commercial and free, provided by public authorities) available, which

⁴⁾ Negatywne konsekwencje korzystania z pornografii, <https://twojasprawa.org.pl/files/attachments/daaf07a3-2d4c-11ea-9e0e-02000025f0dd/raport-sts-badania-naukowe-o-pornografii.pdf> [accessed 16 March 2026]

⁵⁾ European Commission Communication ‘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/PL/TXT/?uri=CELEX%3A52022DC0212> [accessed 16.03.2026]

parents can use to monitor their children's and teenagers' online activity more effectively.

Given the significant amount of pornographic content on the internet, which poses a threat to the healthy development of minors, and the need to ensure an equal level of protection for minors regardless of whether their parents and legal guardians use parental control tools or not, it has been recognised that the measures taken to date have proved insufficient. Although parental control tools are widely available on the market, research by NASK-PIB shows that the majority of respondents are either not interested in them or are unable to use them to monitor their children. The selective use of such tools by individual children or parents is already preventing the economies of scale intended by the legislator from being achieved. Therefore, it is necessary to supplement the actions described above with the introduction of legal regulations.

The main aim of the draft bill is to impose obligations on providers of electronic services which will significantly reduce the possibility of minors gaining access to pornographic content. Even a partial reduction in the availability of pornographic content will constitute a significant improvement in the current situation, where minors are not protected in any meaningful way. In the prevention of pornography addiction, the most important thing is to delay a child's first exposure to pornography, so that very young children do not accidentally come into contact with pornographic material which, due to its high level of content that is incomprehensible to them, has a particularly damaging effect on their mental health.

It should be noted that the draft bill provides for the protection of persons until they reach the age of 18. The rationale behind providing protection against pornographic content for those under the age of 18 is linked to the developmental stages of young people, whose mental development is still very much in progress up to the age of 18, and indeed even beyond into their early adult years. A major problem at present is young people's addiction to pornography, which contributes to the development of dysfunctional behaviours that are then carried over into their adult lives. The root cause of this problem is unrestricted access to pornographic content. It is also worth noting that the nature of pornographic content has changed significantly over the years. This content is no longer purely erotic in nature; increasingly, it depicts violence, the humiliation of women and other socially unacceptable behaviour, which a young person deriving their knowledge exclusively from pornographic films may come to regard as the norm in the sexual sphere. Content of this kind has a significantly negative impact on children's mental health, leading them to imitate inappropriate behaviour, replicate patterns that are dangerous to themselves and others, and causing emotional problems such as anxiety, depression, low self-esteem and a tendency towards risky behaviour. Consequently, the service provider will be required to implement an age verification mechanism if the service contains pornographic content.

It is also important to note that older age groups among young people are showing an increasing interest in pornography. Research by NASK-PIB indicates that, according to 30% of 16-year-olds, their peers view pornographic content online at least once a day, whilst slightly over 20% view such content several times a day. Such frequent contact with pornographic content may be a sign of existing addictions. It is also worth noting that the Convention on the Rights of the Child extends its provisions to persons under the age of 18, recognising that persons of this age require special protection, with a view to their proper development, their social, spiritual and moral well-being, and their physical and mental health.

Given the easy availability of pornographic content, the statistically low average age at which minors first encounter such content, the negative impact on minors' development as documented by research, and the highly addictive nature of such content, it was deemed appropriate to introduce restrictions on access to pornographic content in the manner provided for by the legislation. Before granting access to a service containing pornographic content, the service provider will be required to implement an age verification mechanism to prevent minors from accessing such content. The age verification mechanism itself cannot be based on self-declaration of age and must be designed in accordance with privacy and personal data protection requirements. The mechanisms used worldwide to verify a user's age include, amongst others:

- 1) confirmation that the user is aged 18 or over via open banking (the full date of birth should not be disclosed);
- 2) photo identification match – users can upload an identity document with a photo, such as a driving licence or passport, which is then compared with the user's photo at the time of upload to verify that it is the same person;
- 3) biometric facial age assessment – the user's facial features are analysed to estimate their age;
- 4) verification using credit and debit cards;
- 5) digital identity portfolios.

The draft bill is based on age verification mechanisms that will make it possible to confirm that a person has reached the age of majority. The self-declaration mentioned above is not an appropriate method. By 'age verification mechanism', the proposer means a mechanism designed to unequivocally establish whether users have reached the age of majority, excluding methods based on users' self-declaration of their age. The provider of electronic services will decide which of the age verification mechanisms will be used in each particular case.

It is worth noting that the European and global solutions analysed by the project initiator do not explicitly specify which age verification mechanism is to be used either, but instead adopt a purpose-based approach – ensuring an

effective barrier to prevent children from accessing pornographic content. At the same time, the draft bill states that the mechanism for verifying age involves, in particular, the use of an electronic attribute certificate confirming age, made available as part of the European Digital Identity Wallet.

In the event of failure to comply with the above obligations, the supervisory authority – the President of the Office of Electronic Communications (Urząd Komunikacji Elektronicznej), hereinafter referred to as ‘the President of the UKE’ – will be empowered to carry out checks, including imposing an administrative fine. This fine may apply to both providers of electronically delivered services and internet service providers. It is envisaged that the maximum penalty should be set at the statutory level in the form of an amount rather than a percentage based on the revenues generated. This is because it will often not be possible to determine the revenue accurately, particularly in the case of entities providing cross-border services. The administrative fine imposed on service providers who fail to fulfil their statutory obligations will range from 10,000 PLN to a maximum of 1,000,000 PLN; this introduces an appropriate limit for the President of UKE to determine the amount of the fine and is consistent with the provisions of the Act of 12 July 2024. – Electronic Communications Act (Journal of Laws, item 1221; 2025, items 637 and 820; and 2026, item 252). The administrative fine will be imposed by way of a decision. The draft also contains provisions setting out the rules governing cooperation between the President of UKE and the Chair of the National Broadcasting Council, hereinafter referred to as ‘KRRiT’, in view of the provisions currently in force under the Radio and Television Broadcasters Law of 29 December 1992 (Journal of Laws of 2022, item 1722, and of 2024, items 96 and 1222), which regulate the obligations of certain service providers offering electronic services with regard to protecting minors from accessing pornographic content. Consequently, with regard to entities providing on-demand audiovisual media services and video-sharing platform providers which are established in Poland and are subject to the supervision of the KRRiT, the powers to classify content made available by a service provider as pornographic, and to take action in the event that the service provider fails to comply with the obligation to implement an age verification mechanism and prevent minors from accessing pornographic content, shall rest with the Chair of the KRRiT.

The President of UKE will maintain a register of domain names providing access to pornographic content on the internet without first employing an age verification mechanism and without preventing minors from accessing such content, hereinafter referred to as ‘the register’. Access to a service listed in the register will be blocked by internet service providers. Entries in the register will be made on the basis of applications submitted or ex officio. In view of the need to ensure that service providers are able to respond appropriately to the planned addition of an internet domain name to the register, and thereby to avoid their service being blocked, the Act provides for a notification procedure. Before entering an internet domain name in the register, the President of UKE will be required to notify the subscriber of the internet domain name of the entity’s failure to comply with its obligations to protect against access to pornographic content. The entry will also be preceded by the President of UKE obtaining an opinion from the Chair of KRRiT or NASK-PIB, depending on the entity concerned by the entry.

The Act will not fully resolve the problem of minors’ access to pornographic content. However, one of the objectives of the Act is to eliminate accidental, unintentional exposure to such content, which accounts for a significant proportion of cases. The Act should also help to ensure that the average age at which minors are first exposed to pornographic content does not fall. It is possible that, given their digital skills, minors may attempt to use technical means to circumvent the provisions of the Act, for example by using a VPN. However, it is worth pointing out that VPN-type tools are usually paid for, which is an obstacle to their use by minors, and free versions of VPNs have capacity limitations. From the date of entry in the register, the registrant of the internet domain name shall be entitled to lodge an objection and, if the objection is rejected, to bring an appeal before the administrative court. If an objection or complaint is upheld, this will justify the introduction of appropriate changes to the register, i.e. the removal of the domain from the register by the President of UKE.

It should be emphasised that the Act provides for the right to object to an entry in the register as a means of protecting the interests of service providers, and should the President of UKE refuse to uphold the objection, an appeal may be lodged with the administrative court. As mentioned above, before entering a domain into the register, the authority will notify the internet domain name subscriber of any failure to fulfil the obligations set out in the Act and of its intention to enter the domain into the register. That entity will be given the right to provide an explanation. At the same time, as indicated earlier and based on the research carried out, and taking into account the activities undertaken in Europe and worldwide, this is dictated by the need to ensure the protection of minors by taking measures limiting access to pornographic content on the internet, since other methods used at the user level and at the terminal equipment level are not sufficiently effective. Bearing in mind the need to ensure that the provisions introduced are proportionate to their purpose, the Act will lay down rules governing the maintenance by

the President of UKE of a register of domain names providing access to pornographic content on the internet without a prior age verification mechanism and without preventing minors from accessing such content, as well as the procedure for proceedings before the President of UKE.

The President of UKE (or Chair of KRRiT) will be required to verify whether the content in question actually constitutes pornographic content. The President of UKE will be able to draw on the support of NASK-PIB in this regard, as an institution with extensive experience in protecting minors from cyber threats. Any decisions cannot be taken automatically, but must be reviewed by the supervisory authority with regard to the nature of the content, in order to avoid so-called ‘excessive blocking’, which would run counter to the purpose of the Act – for example, in the case of educational or scientific content. It should be pointed out that, thanks to the case-law of the ordinary courts issued on the basis of the provisions of the Criminal Code Act of 6 June 1997 (Journal of Laws 2025, items 383, 1818 and 1872) and the Radio and Television Broadcasters Law of 29 December 1992, the concept of pornographic content is well established in the Polish legal system, thus the boundary between pornographic content and other content, including, for example, educational content, is clear.

NASK-PIB’s remit will include analysing risks relating to children’s online safety and issuing relevant statements.

The measures taken to date to protect minors from accessing inappropriate content online, including educational campaigns aimed at parents, require support in the form of legal obligations imposed on the aforementioned service providers. Relying solely on parental control tools also fails to yield any tangible results, as the optional solutions offered by, amongst others, electronic communications service providers are subject to a charge and, furthermore, require the minors’ legal guardians to carry out appropriate – and often complex – configurations. The use of such tools by only some parents and legal guardians means that the level of protection of minors from inappropriate content varies, and some minors, as research shows, are not protected at all.

The fulfilment of the obligations imposed on service providers in relation to the use of an age verification mechanism where pornographic content is present in a service may potentially involve service providers gaining access to the personal data of individuals using that service provider’s services. Where a service provider employs an age verification mechanism to grant access to pornographic content, the data collected for the purposes of that age verification mechanism may not be used for purposes other than those specified in this Act, as the general rules on the protection of personal data will apply set out in Regulation (EU) (EU) 2016/679 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 (General Data Protection Regulation) (OJ EU L 119, 15 April 2016, p. 1, as amended), hereinafter referred to as the ‘GDPR’. Therefore, any data processed by a service provider using the age verification mechanism, which serve this purpose and are used by the implemented mechanism, cannot be processed for any other purpose than the application of the age verification mechanism. The Act does not prohibit a service provider from processing data on the legal grounds specified by that provider and provided for in the GDPR. The service provider should therefore not combine data obtained under the age verification mechanism in place with other data held by the service provider. The premise of the Act is to ensure that the processing of personal data as part of the age verification mechanism complies with the principles of personal data protection, in particular the principle of data minimisation, is proportionate to the purpose for which it is intended, and respects the service user’s right to privacy. It should also be emphasised that the provisions of the Act do not provide for the possibility for public administration bodies to access the data of an identified person using a service offered by a service provider falling within the personal scope of the Act. Furthermore, provision has been made for the introduction of a provision requiring the President of UKE to notify the President of the Personal Data Protection Office, hereinafter referred to as the “President of the UODO”, of any doubts regarding the compliance of the age verification mechanism used by a service provider with personal data protection regulations.

The processing of personal data in breach of security requirements may result in unauthorised persons gaining access to personal data (due to data leaks or other disclosure of the identity of a specific person). The role of every data controller processing data in connection with the age verification mechanism is to ensure that safeguards in line with the GDPR are in place. The safeguards necessary for implementation depend on the selected age verification mechanism and the organisational and technical conditions of the service providers. In the event of a data breach, as indicated above, every individual will be entitled to exercise their rights under general legislation, including data protection legislation.

At the same time, there is no need to define a service containing pornographic content, nor to define pornography itself. In Polish criminal law, as well as in the Broadcasting Act of 29 December 1992, the concept of pornographic content appears but has not been deliberately defined by the legislator. The legislature has left it to the courts to determine what, in the circumstances of a particular case, constitutes pornography subject to legal sanctions.

3. How has this problem been solved in other countries, in particular OECD/EU Member States?

Federal Republic of Germany

In the Federal Republic of Germany, according to the provisions of the Inter-Federal Treaty on the Protection of Minors in the Media (in German: Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien – JMStV), access to pornographic content is restricted to adults only. In accordance with Section 184 of the Criminal Code (in German: Under the German Criminal Code (Strafgesetzbuch – StGB) and Section 4(2)(1) of the JMStV, the dissemination of pornography in the mass media is prohibited under pain of criminal sanctions. Websites which provide access to pornographic content are required to adopt appropriate mechanisms to verify the age of users of such sites. Compliance with the age verification rules is checked by the body set up pursuant to the provisions of Section 14 of the JMStV, i.e. the National Commission for the Protection of Minors in the Media (in German: Kommission für Jugendmedienschutz – KJM). It is its responsibility to check whether the provider of the content in question has duly complied with its obligation to label the age category of the individual content and to verify the user's age. Where a breach of this obligation is established, network access providers are required, on the basis of a decision by the KJM, to block access to specific websites by means of blockage at the Domain Name System (DNS) level (i.e. by preventing all internet users who use these providers' services from accessing such a website). Based on a judgment of the competent court, suppliers operating outside the Federal Republic of Germany are also subject to the aforementioned obligation. The Treaty applies to all 'telemedia' (broadly defined as electronic information and communication media) and broadcasting services within the meaning of German law; it therefore also applies to websites and applications. However, over-the-top (OTT) services, including instant messaging, are not explicitly subject to this obligation.

The Act on the Enforcement of Law on the Internet (in German: Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken- Netzwerkdurchsetzungsgesetz – NetzDG), which came into force on 1 October 2017, imposes an obligation on service providers and social media platforms to establish an effective and transparent procedure for handling complaints regarding illegal content and to remove content that is 'manifestly illegal' within 24 hours of being notified. This obligation applies to portals with more than 2 million users.

Similar provisions are contained in the Act of 6 May 2024 on Digital Services (in German: The Digitale-Dienste-Gesetz (DDG) which transposes the provisions of the Digital Services Act (DSA) into German law. It also applies to digital services, which are not audiovisual media services, regulated by the legal acts described above. Thus, the scope of the term includes some portion of digital activity, especially content made available on social networks.

French Republic

On the basis of the Law on the Protection of Victims of Domestic Violence (in French: Loi n° 2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales), as amended on 30 June 2020, ARCOM (in French: Autorité de régulation de la communication audiovisuelle et numérique), the national audiovisual and electronic communications regulator, has the power to conclude that websites providing pornographic content have not put in place proper age verification mechanisms. At present, under French law, a user's declaration that they are over 18 years of age, made solely by ticking the relevant box on a webpage, is not a sufficient mechanism. ARCOM may apply to a court for an order obliging internet access providers to block access to specified websites that fail to comply with the above obligation. Article 23 of the above-mentioned Act concerns all online communication services, including websites and apps (but not the exchange of private correspondence). The law also refers to 'pornographic content', but does not define it.

The Act of 2 March 2022 on strengthening parental control over methods of access to the Internet (in French: LOI n° 2022-300 du 2 mars 2022 visant à renforcer le contrôle parental sur les moyens d'accès à internet) introduced an obligation to equip terminal devices (with operating systems, marketed on the French market) with tools to limit or control minors' access to content that may be harmful to their development. These devices include, amongst others, computers, smartphones, tablets, televisions (Smart TVs) and video game consoles (but, as mentioned, only those with an operating system installed). It is, however, provided that the Act must be supplemented by provisions setting out the functions and technical specifications of parental control devices, as well as the procedures for monitoring compliance with the obligations laid down in this Act.

A decree setting out the functions and technical specifications was adopted in 2023. The decree regulates the technical characteristics of parental control tools, the procedure for their certification, and the obligations of manufacturers and distributors – including information obligations. In accordance with the minimum requirements set out in the decree, the tools are designed to block access to pre-installed or downloaded content (available from app stores) that is unsuitable for minors. This includes, amongst other things, content that is pornographic, relates to gambling or violence, is prohibited by law for persons under the age of 18, or which the publisher has specified as potentially unsuitable for minors. Activation of the tools is to be at the discretion of the user (parent) and must not require the creation of an account. The decree requires manufacturers to inform users (in paper or electronic form) of the risks associated with using the device, for example in relation to addiction, violence or inappropriate content.

On the issue of legislative work on age verification solutions, in February 2023, the French Minister responsible for digitalisation announced that a 'digital certificate' was being developed to verify the age of users online. Closed-door testing of the system was due to begin in March 2024, with its roll-out scheduled for September 2024. According to the minister's statement, the system will operate on the principle of 'double anonymity' – meaning that it will protect the identity of people over 18 when verifying age requirements. According to the minister, the

aim of the new programme is ‘not only to solve the problem of age verification for pornographic websites, but also to potentially extend age verification to other services in the future’.

On 22 May 2024, the Act of 21 May 2024 on securing and regulating the digital space entered into force (in French: Loi n°2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique — SREN). This law is the result of the alignment of national legislation with the DSA and the Digital Markets Act (DMA), as well as parliamentary work on protecting minors from exposure to pornographic content, reports on digital sovereignty, consultations within the Conseil national de la refondation, and initiatives undertaken to regulate the activities of influencers. The law contains certain elements that go beyond the scope of EU regulations.

The provisions of the SREN expand upon those of the 1978 Law on information technology, files and freedoms (in French: Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés). It introduces a principle stating that matching personal data to a person's online activity is deemed to constitute the monitoring of the behaviour of data subjects. It covers data controllers or data processors established outside the European Union which do not supply goods or services to individuals in the country, but process the personal data of individuals in the country. The law provides for the blocking and removal from the register of, and the imposition of heavy fines on, pornographic websites that fail to effectively verify the age of their users, despite this obligation being imposed on them by the law of 30 July 2020 on the protection of victims of domestic violence. The regulations pay particular attention to the issue of Child Sexual Abuse Material (CSAM) and oblige the hosting service provider to remove such material within 24 hours from the date of notification. The SREN regulations provide for a penalty of up to one year's imprisonment and a fine of up to 250,000 euros for web hosting providers (French: les hébergeurs) who fail to comply with their obligation to block such websites. Furthermore, Article 6 (paragraphs II and III) of the SREN Act directs web browser providers to implement measures to block, as a matter of obligation, websites included on a list provided by the government. There are also many critical voices. According to the Mozilla Foundation, this move will overturn the current practice of content moderation standards.

Italian Republic

On 15 September 2023, the Italian government adopted the so-called Caivano Decree (Italian: Il decreto Caivano) (13 November 2023: the decree was adopted by the Parliament of the Italian Republic and became a law (Italian: legge)). In addition to issues relating to the safety of minors and the introduction of additional measures concerning violence against minors, this decree also implements educational measures regarding the presence of children and young people in cyberspace, particularly with regard to pornographic and harmful content. Article 13 of the decree provides the legal basis for the use of parental control applications on the terminal devices of underage users (a fairly broad, exhaustive list, including IoT devices) and obliges service and equipment providers to inform users of the availability or, in certain cases, the necessity of using such solutions. In particular, Article 13-bis introduces restrictions on access to websites with pornographic content, in particular the introduction of effective methods of age verification. However, these have not been clearly defined, and the method or technical measures themselves are to be developed at a later date by the competent authorities. These methods are to be developed in collaboration with the sector. Furthermore, the aforementioned decree established a digital services coordinator in Italy, in accordance with the provisions of the DSA; this role was assigned to ANCOM (Italian: Autorità per le Garanzie nelle Comunicazioni).

The ANCOM regulator mentioned above has strengthened the protection of underage users against harmful content on the internet. Resolution (Italian: delibera) 298/23/CONS, adopted as a result of the public consultation initiated by Resolution 76/23/CONS, sets out the procedures under which ANCOM may act to restrict the dissemination of video material: ‘programmes’, ‘user-generated videos’ or ‘audiovisual commercial communication’ that, as a result of ongoing proceedings, are found to be harmful to the physical, mental or moral development of minors, or that incite racial, sexual, religious or ethnic hatred, or that offend against human dignity. The regulations described above entered into force on 8 January 2024.

As far as age verification is concerned, work on appropriate solutions began a few years ago. The Italian Data Protection Authority GDPD (Italian: Garante per la Protezione dei Dati Personali), at the EDRI (European Digital Rights) forum in 2021, put forward several proposals for the introduction of a digital identity that could be used by all internet users, and in particular by users of social media platforms. Two of the three proposed methods are based on the use of an electronic identity card (eID) – (SPID – Sistema Pubblico di Identità Digitale). The eID solution would also be available for minor users.

In the first scenario, parents or legal guardians would receive a one-off code/password/token generated via eID, and would pass this on to the minor, who could then use it to confirm their age, for example when registering for a social media account. The second option would allow minor users (from the age of 13) to access a temporary SPID account, which, however, would be managed by their parents or legal guardians as administrators. By contrast, the latest proposal is based on the AI-powered age verification tools already implemented by TikTok, which do not rely on public administration services.

According to representatives of the GDPD, public authorities would not have access to information about users, including internet traffic (IP addresses, websites visited and details of their use, etc.). Of course, this would not apply to the competent authorities and services exercising their powers in accordance with national security

regulations and other relevant legislation.

United Kingdom of Great Britain and Northern Ireland

The Online Safety Act 2023, which came into force on 26 October 2023, is expected to become fully effective in 2026 at the latest.

One of the main aims of the Act is to protect users from illegal material posted online (all platforms are required to actively monitor and remove such content) and to protect minors from material that, whilst legal, is harmful (e.g. content encouraging suicide or self-harm).

The Act applies to a wide range of websites, apps and other services, including social networks such as Facebook, Twitter, Instagram, TikTok, etc., as well as cloud storage websites, video-sharing platforms, online forums, dating services and instant messaging services.

A number of services are excluded from the scope of the Act. This includes, amongst other things, emails, SMS/MMS messages, services consisting solely of comments or opinions on published content, news websites, services provided by regulated educational institutions, and services used internally by companies.

The Act sets out a catalogue of priority harmful content, including pornography, suicide-promoting content, self-harm-promoting content, content promoting eating disorders or related behaviour. Reference was also made to content that is offensive on the grounds of, amongst other things, race, religion or sexual orientation; content inciting hatred towards specific individuals; content promoting serious violence against other people; content depicting real or realistic violence against other people and animals, as well as fictional characters; content promoting dangerous ‘challenges’, or encouraging the consumption of dangerous substances, etc.

Providers of user-to-user services (services provided between users, i.e. companies that enable users to share content online or interact with one another, even if the companies providing them are based outside the UK) will be required to carry out a risk assessment regarding the safety of children online (to assess the nature of the content being published, whether it is harmful to minors, and whether minors have potential access to it) and to provide safety measures for these users. Similar obligations apply to search engine providers.

Separate obligations have also been introduced for providers of pornographic content, offering access to such content on their websites. Age verification is mandatory for these websites.

Content is deemed to be pornographic if it is of such a nature that it is reasonable to assume it was produced solely or principally for sexual purposes. Content, as defined by the Act, is anything transmitted via an internet service, whether publicly or privately, including written material or messages, spoken communications, photographs, videos, visual images, music and data of any kind.

The Online Safety Act grants a number of new powers to the UK regulator, Ofcom. In the event of non-compliance with the provisions of the above-mentioned Act, Ofcom may impose a maximum fine of up to €18 million, or even up to 10 % of annual global revenue. The provisions also introduce criminal sanctions against cybercriminals. In the event of failure to comply with its obligations, Ofcom may apply to a court to restrict access to the internet service of a particular provider. In practice, blocking is envisaged at the DNS level.

United States of America

During the proceedings of both houses of the United States Parliament – the House of Representatives and the Senate – numerous bills were tabled which ultimately failed to secure majority support. From time to time, however, draft versions of these bills resurface in the United States Congress.

The Children’s Online Privacy Protection Act (COPPA) is regarded as the most important federal law currently in force in the United States of America concerning the protection of minors from harmful content. The Act, enacted in 1998, came into force on 21 April 2000. COPPA applies to the collection and processing of personal data online by persons or entities subject to the jurisdiction of the United States of America in relation to children under the age of 13, including children outside the United States of America, if the website or service is based in the United States of America. COPPA sets out in detail what a website operator or provider should include in its privacy policy, when and how to seek verifiable consent from a parent or guardian, and what obligations the operator has regarding the protection of children’s privacy and safety online, including restrictions on profiling and marketing to users under the age of 13. With regard to harmful content, COPPA requires all providers of material harmful to minors to restrict minors’ access to their websites. ‘Material harmful to minors’ has been defined as content which, according to general social standards, is regarded as appealing to – in the literal sense – „prurient interest”). This refers to content depicting not only sexual acts but also nudity.

The amended Children and Teens Online Privacy Protection Act, informally known as COPPA 2.0, together with another bill, the Kids Online Safety Act (KOSA), are collectively known as KOSPA (Kids Online Safety and Privacy Act), were passed on 30 July 2024 by the United States Senate. The projects must still be submitted to a vote in the House of Representatives. Under the proposals, online platforms will be required to take measures regarding the design and operation of services used by minors (up to the age of 16) in order to prevent and mitigate harm that may result from such use (e.g. sexual exploitation, online harassment and harmful content, such as the promotion of suicide, eating disorders and drug use). Under the provisions of KOSA, platforms will also be required

to submit annual reports on the foreseeable risk of harm to minors arising from the use of the platforms.

However, given the internal political system of the United States of America, the laws enacted by the individual states of the United States of America are of immense importance.

Louisiana became the first state to pass a law in 2022 requiring websites with at least one-third adult content to verify the age of their users to ensure that none of them is less than 18 years old. Within a few months, other states followed suit (e.g. Texas – Securing Children Online through Parental Empowerment Act – SCOPA, Kansas, etc.), introducing age verification requirements not only for adult websites but also for social media platforms.

In 2022, the State of California prepared a bill to strengthen the privacy of minors' personal data (California Age-Appropriate Design Code Act – CAADCA), which was initially due to come into force on 1 July 2024. One of its objectives was to extend the definition of a child to all persons under the age of 18. The CAADCA requires businesses in the electronic services sector to 'estimate the age of child users with a reasonable degree of certainty'. Furthermore, the CAADCA was intended to apply to companies providing services which children may have access to, but which are not aimed at them (e.g. websites containing pornographic content). The bill, signed by the Governor of California in 2022, was blocked in September 2023 by a federal court on the grounds that it might infringe the First Amendment to the Constitution of the United States of America.

4. Entities affected by the draft

Group	Size	Data source	Impact
The President of UKE	1	Act of 12 July 2024 – Electronic Communications Act	The President of UKE is the regulatory authority for the electronic communications services market. The powers of the President of UKE are being extended to include monitoring service providers' compliance with the provisions of the Act and maintaining a register of domain names that provide access to pornographic content without first carrying out age verification and without preventing minors from accessing such content.
Providers of electronic services	approx. 130 000 (as at 25 November 2024)	Centralna Ewidencja i Informacja o Działalności Gospodarczej [Central Register and Information on Economic Activity], Krajowy Rejestr Sądowy [National Court Register]	Obligation to implement an age verification mechanism when providing access to pornographic content.
Internet access service providers	3821	The Register of Telecommunications Operators maintained by the President of UKE	Blocking access to domains listed in the register.
Minors (0-17 years of age)	6.74 million (6 745ys.) (as of 31 December 2024 – persons of pre-working age up to the age of 18)	Główny Urząd Statystyczny (Statistics Poland) data	Limiting the exposure of minors to pornographic content.
Adults (aged over 18)	30.74 million (30 744 130) (as at 31 December 2024 – persons over 18 years of age)	Główny Urząd Statystyczny (Statistics Poland) data	The introduction of a mandatory age verification mechanism for users of pornographic websites.
The President of UODO	1	the Act of 10 May 2018 on the protection of personal data (Journal of Laws of 2019, item 1781, and of 2026, items 252 and 548)	The President of UODO will receive notifications from the President of UKE whenever the latter has doubts as to whether the age verification mechanism

			used by a service provider complies with personal data protection legislation.
NASK-PIB	1	Regulation of the Council of Ministers of 7 June 2017 on granting the Scientific and Academic Computer Network the status of a state research institute (Journal of Laws 2017, item 1193)	NASK-PIB will be required to issue opinions on whether content made available by a service provider should be classified as pornographic, and on whether the service provider has failed to comply with its obligation to implement an age verification mechanism. Analysing risks to children's safety and publishing announcements.
Administrative courts	17 (16 provincial courts and the Supreme Administrative Court)	The Act of 25 July 2002 Law on the system of administrative courts (Journal of Laws of 2024, item 1267)	The processing of complaints from providers of electronic services regarding the rejection of their objections to the entry of a domain name in the register, and of complaints from such providers and telecommunications operators regarding decisions by the President of UKE on the imposition of financial penalties. In the case of the Supreme Administrative Court, the consideration of appeals against rulings by administrative courts in cases concerning complaints by providers of electronically supplied services regarding the refusal to uphold an objection to the entry of a domain name in the domain name register, and complaints against decisions of the President of UKE.
Chair of KRRiT	1	Radio and Television Broadcasters Law of 29 December 1992	Supervision of entities providing on-demand audiovisual media services and video-sharing platform providers with regard to their obligations concerning the implementation of age verification mechanisms and preventing minors from accessing pornographic content, and cooperation in this regard with the President of UKE.

5. Information on the scope, duration, and summary of consultation results

Since April 2024, an informal working group on the protection of minors from harmful online content has been operating under the Ministry of Digital Affairs. The working group brings together a wide range of institutions and organisations, including representatives of public administration, academic institutions and non-governmental organisations (such as foundations and associations working in the field of child protection). The aim of the group was to conduct a broad discussion and develop recommendations on the appropriateness of introducing regulations in this area. The group's work resulted in specific recommendations regarding legislation to protect minors from accessing harmful content online, particularly pornographic material.

In accordance with Article 5 of the Act of 7 July 2005 on lobbying activities in the legislative process (Journal of

Laws of 2025, item 677, and of 2026, item 160), the draft regulation has been published in the Public Information Bulletin on the Government Legislation Centre's website, on the 'Government Legislative Process' portal, and in the Public Information Bulletin on the website of the Minister responsible for digitalisation.

The draft bill was subject to a 30-day public consultation with the following entities:

- 1) Polska Izba Informatyki i Telekomunikacji [Polish Chamber of Information Technology and Telecommunications];
- 2) Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji [National Chamber of Commerce for Electronics and Telecommunications];
- 3) Polska Izba Komunikacji Elektronicznej [Polish Chamber of Electronic Communications];
- 4) Krajowa Izba Gospodarcza [National Chamber of Commerce];
- 5) Krajowa Izba Komunikacji Ethernetowej [Polish Chamber of Ethernet Communication];
- 6) Polska Izba Radiodfuzji Cyfrowej [Polish Chamber of Digital Radio Broadcasting];
- 7) Polska Izba Handlu [Polish Chamber of Commerce];
- 8) Izba Gospodarki Elektronicznej [Polish Chamber of Digital Economy];
- 9) Krajowa Izba Gospodarki Cyfrowej [National Chamber of Digital Economy];
- 10) Polskie Towarzystwo Informatyczne [Polish Information Processing Society];
- 11) Stowarzyszenie Inżynierów Telekomunikacji [Polish Association of Telecommunication Engineers];
- 12) Fundacja Panoptykon ['Panoptykon' Foundation];
- 13) Związek Pracodawców Mediów Publicznych [Association of Public Media Employers];
- 14) Związek Pracodawców Mediów Elektronicznych Mediakom [The Mediakom Association of Electronic Media Employers];
- 15) Związek Pracodawców Branży Internetowej IAB Polska [Interactive Advertising Bureau Poland];
- 16) Związek Telewizji Kablowych w Polsce Izba Gospodarcza [Cable Television Association in Poland, Chamber of Commerce];
- 17) Związek Cyfrowa Polska [Digital Poland Association];
- 18) Sektorowa Rada ds. Kompetencji – Telekomunikacja i Cyberbezpieczeństwo [Sectoral Skills Council – Telecommunications and Cybersecurity];
- 19) Polska Rada Biznesu [Polish Business Council];
- 20) Naczelna Organizacja Techniczna [Polish Engineering Association];
- 21) Stowarzyszenie Twoja Sprawa ['Your Cause' Association];
- 22) Fundacja Dajemy Dzieciom Siłę ['We Give Children Strength' Foundation];
- 23) Towarzystwo Przyjaciół Dzieci [Society of Friends of Children];
- 24) Save the Children International Poland Foundation;
- 25) Centrum Edukacji Obywatelskiej [Centre for Civic Education];
- 26) Fundacja Szkoła z Klasą ['School with Class' Foundation].

The following entities were asked to present within 30 days their opinions on the draft bill:

- 1) Krajowa Rada Radiofonii i Telewizji [The National Broadcasting Council];
- 2) Prezes Urzędu Ochrony Konkurencji i Konsumentów [President of the Office of Competition and Consumer Protection];
- 3) Prezes Urzędu Komunikacji Elektronicznej [President of the Office of Electronic Communications];
- 4) Prezes Urzędu Ochrony Danych Osobowych [President of the Personal Data Protection Office];
- 5) Rzecznik Małych i Średnich Przedsiębiorców [Ombudsman for Small and Medium-Sized Enterprises];
- 6) Komisja Nadzoru Finansowego [The Polish Financial Supervision Authority];
- 7) Rzecznik Praw Dziecka [Ombudsman for Children];
- 8) Rzecznik Praw Obywatelskich [Ombudsperson];
- 9) Prezes Głównego Urzędu Statystycznego [President of Statistics Poland (GUS)];
- 10) Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy [Scientific and Academic Computer Network – National Research Institute];
- 11) Chairman of the State Commission on Counteracting the Sexual Exploitation of Minors under the age of 15.

Furthermore, the following entities were requested to provide their opinions on the draft Act, with a deadline of 30 days for submission, in accordance with Article 16 of the Act of 23 May 1991 on employers' organisations (Journal of Laws of 2025, item 423) and Article 19 of the Act of 23 May 1991 on Trade Unions (Journal of Laws of 2026, item 549):

- 1) Business Centre Club Union of Employers [Związek Pracodawców – Business Centre Club];
- 2) Pracodawcy Rzeczypospolitej Polskiej (Employers of the Republic of Poland);
- 3) Confederation Lewiatan [Konfederacja Lewiatan];
- 4) Związek Przedsiębiorców i Pracodawców [Union of Entrepreneurs and Employers];
- 5) Związek Rzemiosła Polskiego [Polish Craft Association];

- 6) Polskie Towarzystwo Gospodarcze [Polish Economic Society];
- 7) Federacja Przedsiębiorców Polskich [Federation of Polish Entrepreneurs];
- 8) Niezależny Samorządny Związek Zawodowy „Solidarność” [‘Solidarność’ Independent Self-Governing Trade Union];
- 9) Ogólnopolskie Porozumienie Związków Zawodowych [All-Poland Alliance of Trade Unions];
- 10) Forum Związków Zawodowych [Forum of Trade Unions].

Following discussions, public consultations and the submission of opinions, significant amendments were made to the draft bill; and, given the scope of these amendments, the revised text of the draft bill was subjected to a further 30-day period of public consultation and the submission of opinions.

The draft bill was submitted for opinion to the Digital Affairs Council, the Social Dialogue Council and the Public Benefit Activities Council.

Bill An opinion on the draft from the Joint Commission of the Government and Local Government is not required, as it does not concern the issues concerning local government, including those defining relations between local government and other public administration bodies.

The results of public consultations and opinions were discussed in the consultation report.

6. Impact on the public finance sector

(fixed prices for 2026)	Impact over 10 years from implementing the amendments [PLN million]											
	0	1	2	3	4	5	6	7	8	9	10	Total (0–10)
Total revenue	0.28	0.63	0.67	0.69	0.71	0.73	0.75	0.76	0.78	0.81	0.83	7.63
state budget	0.00	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.19
local government units	0.03	0.09	0.09	0.10	0.10	0.10	0.11	0.11	0.11	0.12	0.12	1.08
National Health Fund	0.05	0.10	0.11	0.11	0.11	0.11	0.12	0.12	0.12	0.13	0.13	1.21
ZUS	0.19	0.40	0.42	0.43	0.44	0.45	0.46	0.48	0.49	0.50	0.51	4.77
Solidarity Fund	0.01	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.23
Labour Fund	0.01	0.01	0.01	0.01	0.01	0.01	0.02	0.02	0.02	0.02	0.02	0.16
Total expenditure	2.56	1.87	1.88	1.91	2.11	2.98	2.14	2.18	2.22	2.38	3.48	25.71
state budget	2.56	1.87	1.88	1.91	2.11	2.98	2.14	2.18	2.22	2.38	3.48	25.71
local government units	0	0	0	0	0	0	0	0	0	0	0	0
other units (separately)	0	0	0	0	0	0	0	0	0	0	0	0
Total balance	-2.29	-1.24	-1.21	-1.22	-1.40	-2.26	-1.40	-1.41	-1.43	-1.57	-2.65	-18.08
state budget	-2.56	-1.86	-1.86	-1.90	-2.09	-2.96	-2.12	-2.16	-2.20	-2.35	-3.46	-25.52
local government units	0.03	0.09	0.09	0.10	0.10	0.10	0.11	0.11	0.11	0.12	0.12	1.08
National Health Fund	0.05	0.10	0.11	0.11	0.11	0.11	0.12	0.12	0.12	0.13	0.13	1.21
ZUS	0.19	0.40	0.42	0.43	0.44	0.45	0.46	0.48	0.49	0.50	0.51	4.77
Solidarity Fund	0.01	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.23
Labour Fund	0.01	0.01	0.01	0.01	0.01	0.01	0.02	0.02	0.02	0.02	0.02	0.16
Sources of financing	All costs incurred by the President of UKE will be funded from budget section 76 – Office of Electronic Communications. All costs for the minister responsible for information technology from section 27 – information technology (including											

	grants). The entry into force of the proposed regulation will constitute the basis for requesting additional funds from the state budget for this purpose. Furthermore, any implications for the budget sections relating to the President of the Personal Data Protection Office (section 10 – UODO), the National Broadcasting Council (section 09 – KRRiT) and the administrative courts (section 05 – Supreme Administrative Court), will not constitute grounds for planning or applying for additional funds from the state budget in the year the Act comes into force or in subsequent years. In the case of the National Broadcasting Council (KRRiT), the amendments introduced by the draft Act are intended solely to clarify the existing obligations under the Radio and Television Broadcasters Law of 29 December 1992. The tasks imposed on the President of UKE under the proposed regulation will necessitate an increase in the expenditure limit set out in section 76 – Office of Electronic Communications – of the annual budget bill. The expenditure of the state budget resulting from the entry into force of the Act foreseen for the years 2027-2037 resulting from the tasks of the President of UKE will amount to PLN 20 129 618.47. These are the expenses of the President of UKE resulting from the entry into force of the Act. These expenditure items relate to the need to create six additional specialist positions, including one managerial position, and to the need to establish and maintain a register. This is due to the scale and scope of the new tasks relating to the maintenance of the register, as well as the monitoring and supervisory tasks imposed on the President of UKE. Analysis of the workload associated with new tasks for the Office of Electronic Communications, hereinafter referred to as ‘UKE’: Assumptions Number of working days per year – 252 Number of hours spent by one employee on their tasks during a working day – 7 Number of leave days per employee per year – 26 Number of sickness days per employee per year – 10 Number of training days per employee per year – 7 Number of man-hours worked per year by one employee – 1 463 Annual man-hours required for tasks in this area (based on the list of key tasks) – 9 190 hours. Calculated number of staff – 6.28 Minimum number of staff positions – 6 List of key tasks First and foremost, it is important to highlight the need to ensure that the necessary staff resources are in place to carry out the new monitoring and supervisory tasks assigned to the President of UKE, relating to: a) the supervision of service providers, including but not limited to: – carrying out inspections of the implementation of the age verification mechanism for service users and, following such inspections: imposing financial penalties, issuing post-inspection recommendations, issuing decisions ordering the rectification of identified irregularities, as well as entering a web domain into the register of domains providing access to pornographic content without prior age verification – if, as a result of an inspection, it is found that the service provider is not fulfilling its obligations regarding the use of the age verification mechanism (the implementation of a significant part of these tasks will require prior administrative proceedings to be conducted) – time required: 1 560 hours per year; b) the upervision of providers of internet access services, including but not limited to: – monitoring compliance with the obligation to block, free of charge, access to websites using domain names entered in the domain name register that provide access to pornographic content without first applying an age verification mechanism and without preventing minors from accessing such content, within 48
--	---

hours of entry in that register – time required: 1 070 hours per year;
– verification of the redirection of internet traffic to a special information page maintained by the President of UKE for domain names entered in the register – time required: 620 hours per year;
– verification of whether, within 48 hours of a domain name being removed from the aforementioned register, access is still possible to websites using that domain name – time required: 520 hours per year;

Further tasks requiring additional resources for UKE are tasks related to:

a) the register of domain names providing access to pornographic content without first applying an age verification mechanism and without preventing minors from accessing such content:

– receiving reports of domain names providing access to pornographic content without first applying an age verification mechanism – time required: 300 hours per year;

– verification of the above-mentioned reports – time required: 1 000 hours per year;

– notifying domain name registrants of the intention to enter a domain into the register – time required: 230 hours per year;

– reviewing the statements of the above-mentioned entities prior to entry in the register – time required: 270 hours per year;

– registration of internet domain names in the register – time required: 230 hours per year;

– notifying domain name subscribers of the entry in the register – time required: 150 hours per year;

– maintaining and updating the register, ongoing cooperation with NASK-PIB and the Chair of the National Broadcasting Council – time required: 800 hours per year.

b) processing objections relating to entries in the register:

– review of objections filed by domain name subscribers, within 14 days of receipt – time required: 450 hours per year;

– informing the party lodging the objection of how it will be dealt with and of their right to bring a complaint before an administrative court – time required: 130 hours per year;

– removal of a domain name from the register – if the objection is upheld – time required: 60 hours per year;

Carrying out the above tasks will require the establishment of a new organisational unit; it is estimated that this will necessitate the employment of 5 full-time staff (including 4 specialist posts and 1 managerial post).

It should be borne in mind that decisions issued by the President of UKE will be subject to appeal before an administrative court. Furthermore, should the President of UKE fail to uphold an objection to the entry in the register of domain names that allow access to pornographic content without prior age verification and without preventing minors from accessing such content, an appeal may be lodged with the administrative court. This entails the need to engage legal services; therefore, one specialist full-time post (legal adviser) will be required – time required: 1 800 hours per year;

The costs include expenses related to:

– the purchase and maintenance of equipment necessary for the operation of the register;

– the purchase and maintenance of the software required to maintain the register (including ensuring access for data entry and the automatic transmission of such data to internet service providers),

– the purchase and implementation of the security systems necessary to prevent data integrity breaches;

– human resources in connection with providing the service and maintaining the register;

– the design of the register, i.e. the design work related to its implementation any subsequent work required to improve the register's operations;

– the general costs associated with the maintenance of the register, which go beyond the costs previously specified.

When estimating the costs of individual components, it was assumed that the register being developed would be part of UKE's IT ecosystem. This means that it will make use of the existing infrastructure, and the costs have been estimated for the essential and additional components required for the system to function properly and to ensure an adequate level of security.

Equipment required to maintain the register:

In order to implement the system for maintaining the register, it is planned to purchase the IT equipment needed to build, run and operate the IT system. This equipment is the technical layer of the solution and enables the proper operation of applications, databases, integration services and security mechanisms.

A purchase worth PLN 800,000 in 2027 can be broken down as follows:

- application and database servers,
- disk arrays or storage systems,
- data backup and recovery equipment.

The expenditure in subsequent years relates to the costs of maintenance, operation and servicing of the infrastructure purchased. It was decided that the hardware infrastructure would be replaced or significantly upgraded every five years, in view of performance considerations and the rising costs of maintaining the existing infrastructure. Furthermore, when estimating costs, account was taken of the fact that, over time, manufacturers may cease or significantly reduce support for certain hardware and software components, which increases the risk of failures and security issues. Provision has also been made for annual funding to subsidise infrastructure upgrades, such as additional network nodes or storage capacity, which exceed the costs of routine system maintenance.

The costs were estimated on the basis of current market prices and similar purchases made by the Office of Electronic Communications.

Software – development of a system for maintaining the register:

Spreading expenditure over two financial years enables the rational management of financial resources and helps to minimise project risk through phased implementation and ongoing monitoring of the results achieved.

Year 2027 – PLN 360 000

During the first year, a number of key project phases are envisaged, including:

- the development of the system, i.e. the creation of the application code and integration components,
- testing and pilot implementation,
- user training.

Year 2028 – PLN 100 000

In the second year, activities are planned related to:

- integration with existing systems,
- the launch of the system into production,
- user training.

The costs were estimated using expert methodology and on the basis of experience in building similar systems.

Security systems:

In 2027, expenditure of 320 000 was foreseen for the purchase and implementation of IT security systems necessary to protect the ICT infrastructure and the data being processed. These expenditure items include, in particular, a firewall, a server security system and the expansion of the centralised security incident monitoring solution. And in 2028, there are plans to expand the data backup and recovery system. The replacement of security systems, mainly firewalls, is planned every 5 years.

	The costs were estimated on the basis of current market prices and similar purchases made at the Office. Design – designing an IT system, in particular: • detailed requirements analysis, • database design, i.e. defining data structures, relationships and the way information is stored, • interface design, i.e. input and output screens and user interface, • system architecture design, i.e. dividing into modules and defining how they should work together, • preparing the project specifications, i.e. setting out all the requirements in a document to be used for implementation. The costs were estimated using expert methodology and on the basis of experience in building similar systems. Maintenance and development Costs relating to software maintenance and development have been budgeted for from 2029 onwards. Maintenance and minor software development are necessary to ensure the business continuity of the IT system and its compatibility with evolving organisational, legal and technical requirements. The system must be continuously adapted to changes in regulations, internal procedures, user needs and integration with other systems. The increase in the level of maintenance in subsequent years is also linked to the termination of the current guarantee periods, the increase in costs resulting from the development support for the older code and the adaptation of the register to the new versions of the operating systems, as well as the natural growth of the register. Costs have been estimated on the basis of maintenance costs already incurred for similar software already in use. Costs related to the creation and maintenance of the register were not included in the general costs related to the creation and maintenance of posts. For the calculation of the costs of increasing employment, uniform assumptions have been made according to which: • the cost of creating one post in 2027 – PLN 18 820 includes: - a one-off purchase of furniture – PLN 3 500, - a one-time purchase of a mobile phone – PLN 150, - a one-off purchase of computer equipment – PLN 10 000, - a one-off purchase of office software (licences) – PLN 5 170, • the annual cost of maintaining one post in 2028 – PLN 8 300.98, includes: - support services and logistics supplies – PLN 1 261.98, - training – PLN 5 125.00 (from 2029, training costs will be reduced to PLN 2 000 per full-time post), - domestic travel – PLN 1 051.65, - annual telephone subscription and internet connection – PLN 862.35; Between 2028 and 2037, the cost of maintaining posts shall be increased by the inflation rate specified for each year in the Minister of Finance's guidelines on macroeconomic indicators. No expenditure is anticipated on the additional annual remuneration (dodatkowe wynagrodzenie roczne, DWR) for the first year of the Act's validity; the first calculation of the DWR for 2027 will take place in 2028. Taking into account the costs associated with filling the post, as described above: • cost of creating 6 posts in 2027 – PLN 119 520 (including occupational health and health and safety costs); • total cost of maintaining 6 posts between 2027 and 2037 – 387 800.38 PLN; • actual cost of 6 specialist posts between 2027 and 2037 – PLN 14 519 618.47 (including the costs of establishing and maintaining posts, without the costs of establishing and maintaining the register), including those derived from the
--	--

	employer (20.88% of the gross amount). A detailed breakdown of UKE's costs is presented in the table attached as Annex 1 to the Regulatory Impact Assessment. The tasks assigned to NASK-PIB will form the basis for NASK-PIB to apply for a specific-purpose grant, up to the amount specified in the Act. A detailed breakdown of the costs is set out in the table in Annex 2 to the to the Regulatory Impact Assessment. The tasks assigned to NASK-PIB stem directly from the obligations set out in Article 12, Article 14(5) and Article 18 of the Act, concerning the issuing of opinions on the classification of content as pornographic, service providers' compliance with their obligations regarding age verification, and the analysis of risks associated with minors' access to pornographic content on the internet and the publication of relevant communications. The expenditure associated with fulfilling these obligations stems primarily from the need to provide specialist staff responsible for analysing online content in order to prepare expert opinions for the President of UKE, and to carry out analytical and information-gathering activities concerning the risks associated with minors' access to pornographic content on the internet. Analysis of the workload associated with new tasks for NASK-PIB: Assumptions Number of working days per year – 252 Number of hours spent by one employee on their tasks during a working day – 7 Number of leave days per employee per year – 26 Number of sickness days per employee per year – 10 Number of training days per employee per year – 7 Number of man-hours worked per year by one employee – 1 463 Annual man-hours required for tasks in this area (based on the list of key tasks) – 2 900 hours. Calculated number of staff – 1.98 Minimum number of staff positions – 2 List of key tasks a) carrying out of the tasks set out in Article 12 of the draft bill: – analysis of the content made available by service providers within the reported domains to determine whether the content found there constitutes pornographic material – time required: 780 hours per year; – assessment of service providers' compliance with the obligation to apply the age verification mechanism referred to in Article 3(1) of the draft bill – time required: 520 hours per year; – preparing and submitting expert opinions to the President of UKE, alongside ongoing working cooperation and the exchange of information – time required: 320 hours per year; b) carrying out of the tasks set out in Article 14(5) of the draft bill: – analysis of the explanations provided by domain name registrants following receipt of a notice of intended entry in the register – time required: 420 hours per year; – re-verification of content made available by service providers and assessment of the mechanisms put in place to restrict minors' access to pornographic content – time required: 300 hours per year; – preparation of expert opinions for the President of UKE, alongside ongoing working cooperation and the exchange of information – time required: 180 hours per year; c) carrying out of the tasks set out in Article 18 of the draft bill: – carrying out analyses concerning the risks associated with minors accessing pornographic content on the internet – time required: 260 hours per year; – preparing and publishing information announcements and expert articles on the
--	--

	NASK-PIB website – time required: 120 hours per year. The implementation of the indicated tasks will require the provision of at least 2 specialist posts ensuring competence in the field of analysis of online content, digital security, the functioning of services provided electronically and the preparation of expert opinions and analyses regarding threats in the digital environment. To calculate the costs of increased labour input, the equivalent of two specialist full-time posts was assumed (the performance of NASK-PIB’s statutory tasks may involve the creation of separate posts or an increase in expenditure on existing posts due to an increase in the duties of those staff members); uniform assumptions were adopted, according to which: - the cost of creating one post in 2027 – PLN 18 820; - annual cost of maintaining one post in 2028 – PLN 8 300.98. No expenditure is anticipated on the additional annual remuneration (dodatkowe wynagrodzenie roczne, DWR) for the first year of the Act’s validity; the first calculation of the DWR for 2027 will take place in 2028. - the cost of creating/adapting 2 posts in 2027 – PLN 37 640; - total cost of maintaining 2 posts between 2027 and 2037 – PLN 129 266.81. The total maximum limit of state budget expenditure allocated to the performance of NASK-PIB’s tasks, on the basis of which NASK-PIB applies for a special-purpose subsidy, amounts to PLN 5 583 154.36 for the period 2027-2037.
Additional information, including the identification of data sources and assumptions made in the calculation	It is envisaged that the register will be maintained by the President of UKE; this body already has obligations regarding the maintenance of registers under separate legislation (e.g. the Act of 12 July 2024 – Electronic Communications Act).

7. Impact on the competitiveness of the economy and entrepreneurship, including the functioning of enterprises and impact on families, citizens and households

Impact									
Time in years since entry into force of the amendments		0	1		2	3	5	10	Total (0–10)
In monetary terms (PLN million, fixed prices for [year])	large enterprises	0	0		0	0	0	0	0
	micro-, small- and medium-sized enterprises	0	0		0	0	0	0	0
	families, citizens and households	0	0		0	0	0	0	0
	(add/remove)								
In non-monetary terms	large enterprises				The aim of implementing an age verification mechanism is to establish whether a user has reached the age of majority and to prevent underage users from accessing pornographic content.				
	micro, small, and medium-sized enterprises (SMEs)				The aim of implementing an age verification mechanism is to establish whether a user has reached the age of majority and to prevent underage users from accessing pornographic content.				
	families, citizens, and households				The proposed legislation will have a positive impact on the safety of children and young people whilst using the internet, by limiting the negative impact of pornographic content on the development of minors.				
Unmeasurable	(add/remove)				To enable the safe use of the internet and ensure the harmonious development of children in terms of digital and sexual education by reducing the percentage of people accessing pornographic content online, particularly their first exposure to pornography at a young age.				

Additional information, including the identification of data sources and assumptions made in the calculation	Impact on entrepreneurs When assessing the impact of the proposed changes, it should be noted that it is impossible to accurately estimate the effects of the regulations in question. The Act imposes new obligations on entities providing services by electronic means, in particular those operating websites and web portals that can be visited by children and young people. Depending on the content uploaded and available on the website, the nature of the service offered and the profile of its recipients, the scope of the obligations imposed by the law may vary considerably. It is not possible to indicate the costs of implementing the age verification mechanism, as it depends on the size of the service (both in terms of the technical organisation of the service and the number of users using it), its nature (including in terms of technical and organisational measures used by the service provider) and the type of content posted on the websites of a given entity. The mechanisms required for implementation may prove to be excessive or unnecessary in cases where service providers do not host pornographic content on their websites, or where they themselves take effective measures to remove such content from their sites or prevent minors from accessing it. In that case, the Act will not give rise to any new obligations or costs. If the website contains pornographic content, it will be necessary to implement an age verification mechanism. This cost is difficult to estimate, as the Act does not set out in detail the mechanism for age verification, but only the requirements designed to ensure that the mechanism operates effectively and that the right to privacy is respected. Consequently, depending on the mechanism chosen by the service provider, the cost of such security measures may vary. With this in mind, it is not possible to identify underlying constants that serve as a reference point in the cost analyses that are conducted. At the same time, the draft bill sets out an example of an age verification mechanism that would fulfil the statutory obligation; this mechanism will be available through the use of the European Digital Identity Wallet, which will significantly reduce the potential costs of implementing such a mechanism.	
8. Change in the regulatory burdens (including disclosure obligations) resulting from the draft		
☐ not applicable		
Burdens are placed outside those strictly required by the EU (see the inverted compatibility table for details).	☐ yes ☐ no ☒ not applicable	
☐ reduction in the number of documents ☐ reduction in the number of procedures ☐ shortening of the time to settle the matter ☐ other:	☐ increase in the number of documents ☐ increase in the number of procedures ☐ extension of the time to settle the matter ☐ other:	
The introduced burdens are suitable for digitisation.	☒ yes ☐ no ☐ not applicable	

Comment:

The relevant regulations will apply to providers of electronic services offering access to pornographic content. They will be required to implement an age verification mechanism to check that users of such websites are of legal age. Entities that fail to comply with the obligations imposed by this Act should be prepared to face the consequences associated with the sanctions provided for therein, such as restrictions on business activities (through the blocking of websites containing pornographic content at DNS level) and financial penalties (of up to 1 million PLN). Furthermore, internet service providers will be required to comply with the obligation to block websites designated by the President of UKE.

It should be pointed out that the issue of children's access to pornographic content online requires urgent regulation, as evidenced by numerous studies showing the scale of minors' access to such content and its negative impact on their development. For this matter, it is therefore justified to introduce additional regulatory burdens without which it would not be possible to increase the safety of minors. By making the age verification mechanism mandatory, the proposed measures offer a practical way of restricting access to this type of content, which is all too common online. Given the unequivocally negative nature of the issue in question, the first step should be to limit initial, often accidental, exposure to pornography. In this case, the obligations will not vary according to the size of the service providers; they will be uniform and apply universally to anyone who provides pornographic content online. It is not justified to differentiate the obligations in terms of the size of the entrepreneurs, as even if an entity meets the criteria of being a micro or small entrepreneur, the impact of its action can be much larger, due to the specificities of the service it provides and the number of recipients of the service. Differentiating obligations in terms of the scope of the entities concerned, or introducing exemptions for certain entities, would result in an uneven level of protection for minors. However, in the case of any entity, the supervisory authority's assessment of the measures taken by that entity will depend on the entity's organisational circumstances and the characteristics of the service it provides.

At the same time, taking into account the principles set out in Article 67 of the Act of 6 March 2018 – Entrepreneurs' Law, in connection with the imposition of the necessary obligations provided for in the proposed act, the project initiator will carry out an assessment of the scope for possible reduction of other burdens resulting from the regulations in force in the field of electronically supplied services.

9. Impact on the labour market

No impact on the labour market is anticipated as a result of the proposed legislation. In the case of the largest portals and websites, it may be necessary to hire specialists to supervise the age verification mechanism.

10. Impact on other aspects

☐ natural environment ☐ regional standing and development ☒ ordinary, administrative or military courts	☐ demography ☐ state property ☐ other:	☒ computerisation ☒ health
---	---	---

Discussion of the impact	The aim of the draft bill is to protect minors from the influence of pornographic content, which can lead to addiction and impair their mental and physical development. A register of domain names that provide access to pornographic content on the internet without first applying an age verification mechanism and without preventing minors from accessing such content will be maintained in an ICT system, which will facilitate compliance with the regulations by entities required by the Act to block such websites. The draft bill introduces administrative penalties for failure to comply with its obligations. It is also envisaged that administrative courts will have jurisdiction in disputes relating to the entry of a specific domain name in the register.
--------------------------	---

11. Planned implementation of the provisions of the Act

The Act provides for a 12-month *vacatio legis*. This is a long enough period to allow service providers to adapt to the new obligations set out in the draft bill.

12. How and when will the impact of the draft be assessed, and what measures will be applied?

It is envisaged that an assessment of the Act's effectiveness will be carried out within four years of the proposed Act coming into force. The primary aim of the draft bill is to restrict minors' access to pornographic content; for this reason, one of the measures of the Act's effectiveness will be the results of surveys on the protection of minors carried out regularly by NASK-PIB, which report, amongst other things, on the percentage of children who report having been exposed to pornographic content. A decrease in this percentage would indicate a positive impact of the

law.

In addition, when assessing the effects of the Act's implementation, the following will be taken into account:

- the number of regulatory interventions and orders to enter domain names in the register,
- the number of objections addressed to the President of UKE,
- the number of reports submitted by third parties to the regulator within the scope of the Act,
- user satisfaction (including that of minors and their parents) with the functioning of the protection system,
- assessment of proportionality – whether the protection mechanisms unduly restrict access to content on the basis of administrative court rulings.

13. Annexes (important source documents, research, analyses, etc.)

1. A detailed breakdown of the costs associated with hiring new staff (a total of 6 full-time posts) in the office supporting the President of the Office of Electronic Communications, and the costs of establishing the register (Annex 1 to the Regulatory Impact Assessment),
2. A breakdown of the costs associated with the award of a specific-purpose grant for tasks carried out by NASK-PIB (Annex 2 to the Regulatory Impact Assessment).