HELLENIC REPUBLIC

Ministry of Digital Governance Διακυβέρνησης

PROTECTING MINORS FROM INTERNET ADDICTION

NATIONAL STRATEGY

HELLENIC REPUBLIC

MINISTRY OF DIGITAL GOVERNANCE

CONTENTS

1. Digital Transformation and Minors

Digital transformation within a country is a process that impacts all aspects of society, including the economy, education, governance, and all social groups. Among these groups, children are significantly affected, as this transformation brings not only new opportunities but also new challenges. Through technology minors gain access to education tools, information and platforms that improve their knowledge and skills. Nevertheless, digital transformation also entails dangers, such as exposure to improper content, breach of privacy, increased potential for online harassment, screen addiction and deteriorating mental health.

Most adults are aware of their moral and legal obligation to educate and protect children from threats to their physical and mental well-being, such as violence and substance abuse. However, adults have not yet developed the same code of conduct nor reflexes when it comes to the digital world, as they are not fully aware of the risks while navigating the online environment. It is now undeniable that children; while using the internet, encounter phenomena ranging from cyberbullying and hate speech to sexual abuse, exploitation, harmful content, and addiction—all of which violate their rights and jeopardize their safety and well-being.

The Ministry of Digital Governance is leading Greece's efforts in the Digital Transformation, implementing digital transition projects that traverse all levels of public administration through increased connectivity, digital skills, accessibility, and use of artificial intelligence. Simultaneously, it implements measures to ensure secure citizen access to information systems, strengthen cybersecurity, and protect children in the digital world. To that end, further to nationwide interventions, there is a need for institutional and regulatory interventions in regional and international organizations, such as the EU, the Council of Europe, the UN, and the OECD, as was recently noted by the Greek Prime Minister at the 79th Session of the UN General Assembly.

In this context, the National Strategy for the Protection of Minors from Internet Addiction was formulated. The Strategy seeks to ensure that Greece's digital transformation delivers maximum benefits to society, particularly for minors, while providing robust protection and access to a safe, creative, and supportive online environment.

1.1. Need for Immediate Intervention and Strategy

Prolonged exposure to digital environments and devices has the potential to adversely affect the developing brains of children, with negative repercussions for their overall health. Such changes are often epigenetic, implying that stress and other environmental factors may result in permanent neurological and health issues. Recent scientific research underscores the particular vulnerability of children to chronic stress, which may precipitate long-term health complications, including an elevated risk of mental health disorders, anxiety, and depression. The unregulated or improper use of digital media exacerbates these risks, fostering a “vicious cycle” of anxiety and diminished capacity to manage daily life.

The impetus behind this National Strategy lies in the need to safeguard minors against the challenges of the digital world and to **provide children and adolescents with a digital environment where their rights are safeguarded and respected**. Digital engagement offers notable opportunities for socialization, education, entertainment, creative expression, and democratic participation. Nevertheless, it is well noted that large social network platforms entail major risks for the health of minors, through intended system design that, for instance, performs user profiling and contributes to screen addiction in children. These activities frequently occur without the knowledge or consent of the children themselves, their parents, or legal guardians.

1.2. Strategic Framework and Action Plan

To facilitate the implementation of this Strategy, an initial comprehensive analysis of the current landscape was conducted, drawing upon the latest and most credible scientific studies. This assessment considered parameters such as modern technologies, online applications, data and metadata processing by digital platforms, profiling mechanisms, and the prevalence of screen addiction. Additionally, it examined the legal and regulatory frameworks at the national, European, and global levels while incorporating insights from exemplary European and international practices.

Following this analysis, the vision and priorities of the Strategy were refined, culminating in the delineation of strategic directions. These directions encompass priorities addressing algorithmic addiction, educational and informational initiatives, and the development of protective measures and mechanisms for minors.

Consequently, an Action Plan was devised, including a comprehensive roadmap and monitoring indicators. The Strategy also defines necessary institutional initiatives, projects for implementation, sources of funding, and processes for monitoring, evaluation, and periodic updates.

2. Internet and Children's Screen Addiction

2.1. Technology and the Internet

2.1.1. Internet Applications and Artificial Intelligence Algorithms

Artificial Intelligence (AI) has emerged as one of the most powerful tools within modern social networks and internet applications, owing to its ability to analyse vast amounts of data in real time, personalize content, and analyse user behaviours and habits. Core techniques include Natural Language Processing (NLP), Machine Learning (ML), and Deep Learning (DL), which are employed across a range of services and functions serving millions of users globally on a daily basis.

Specifically, the personalization of content and the real-time generation of recommendations for suitable and tailored content on large online platforms and social networks is currently achieved using AI models Deep Learning algorithms which analyse user behaviour in real time and provide related content, videos and products, thus increasing user dedication, offering infinite scrolling through relevant content, and increasing the likelihood of purchases, ad engagement, or use of other applications. Such techniques are extensively deployed by platforms like Facebook, Instagram, TikTok, and YouTube and rely on both supervised and unsupervised learning, constantly evolving and improving through new data and self-training methods.

At the same time, the dynamic construction of personalized user profiles, even when not logged-in in an user account, enables platforms to assess and analyse behaviours, moods, sentiments, and more broadly, monitors users' preferred content and interactions with content or other users. **Social networks leverage AI technologies, such as sentiment analysis and natural language processing (NLP), to interpret users' attitudes and opinions.** Sentiment analysis allows platforms to identify how users react to visual content (e.g., images, videos), news, or products, while NLP detects user responses (e.g., comments), opinions, behaviours and habits.

2.1.2. Personal Data and Metadata Use

Social networks, online platforms and applications rely heavily on the collection and processing of personal data from users, even when they are not logged into user accounts to provide personalized services, enhance user experience, and support targeted advertising models. While these practices offer convenience to users, they raise significant concerns regarding privacy protection, data security, and the ethical use of personal information, particularly for minors. Specifically, the collection of personal data—including preferences, locations, demographic details, and browsing history—enables platforms to craft tailored user experiences that increase engagement, time spent online, and the likelihood of purchases through advertisements. **Advertising companies collaborate with social media to obtain precise information about user preferences and behaviours, enabling the targeting of specific audiences, age groups, and user profiles.** However, these practices raise concerns about how personal data is monetized by companies, particularly in the case of excessive internet use among minors leading to screen addiction and adverse effects on mental health.

2.1.3. Personalisation Mechanisms for Minor Users and Screen Time

Personalization, through profiling mechanisms, of minors using the internet and social networks is a critical issue, as it directly impacts their privacy, mental health, and online safety. As already mentioned, social networks apply personalized profiles to users, including children, to adapt content to their preferences. Children are particularly vulnerable to these methods, where their data is used to effectively manipulate them, increase screen exposure and, ultimately, screen addiction. Screen time and exposure to online applications among minors are continuously and rapidly rising due to greater internet access through mobile devices, with social network usage becoming an integral part of their daily lives. According to a 2020 UNICEF Report, approximately one-third of global internet users are under the age of 18. Platforms such as TikTok, Instagram, Snapchat, and Facebook are increasingly popular among minors, while over 80% of children consume content on YouTube. These platforms have become, for many young users, the primary means of communication and information, replacing traditional forms of media and news. **Consequently, profiling on minors has serious implications, as their personal data can be used to create profiles that affect their decisions and preferences.** Given they are at a critical developmental stage, minors are particularly vulnerable to peer pressure and promotional tactics of digital marketing while screen addiction poses a serious threat to their overall health and well-being.

2.1.4. Addiction and Health Impacts

The increased exposure of minors to screens has raised significant concerns regarding its impact on their health and development. A recent report of the World Health Organisation[1] underscores the need for more reasonable internet use by children, highlighting the problematic nature of social media use, linking it to symptoms of addiction. These symptoms include an inability to control the duration of online activity, neglect of other responsibilities or activities in favour of screen interaction, and engagement with digital platforms.

Recent scientific studies further indicate that extensive use of digital devices adversely impacts minors' mental and physical health, as well as their social lives. Extended screen time and use of internet applications are linked to heightened anxiety, depression, and sleep disorders in children and adolescents. Screen addiction also contributes to mood swings and difficulties in emotional regulation. Excessive use of social networks fosters unhealthy comparisons with peers, often leading to negative emotions and diminished self-esteem. **Children spending more than two hours daily on screens face an increased risk of developing symptoms of depression and anxiety, driven by the pressure to meet social expectations and comparisons.** The continuous flow of news, social comparisons, and the pressure to gain more “likes” and acceptance from others significantly disrupt their emotional well-being.

The use of devices before bedtime negatively affects sleep quality, impacting both physical and mental health. Blue light emitted by screens inhibits melatonin production, a hormone essential for sleep, resulting in delayed sleep onset and reduced sleep duration and quality. Studies indicate that children using electronic devices for at least one hour before bedtime are 60% more likely to experience **sleep disorders,** such as insomnia or excessive daytime sleepiness.

A sedentary lifestyle associated with excessive digital device usage also contributes to increased rates of **childhood obesity and chronic conditions**, such as Type 2 diabetes and cardiovascular issues. Research indicates that children spending more than 2–3 hours per day on screens are less physically active, leading to weight gain. Screen addiction can also adversely affect vision, with prolonged exposure to screens at close distances causing **dry eye syndrome** and increasing rates of **myopia** in children.

Lastly, excessive use of digital devices **hampers the development of social skills** in children. The replacement of face-to-face interactions with online communication reduces opportunities to cultivate empathy and interpersonal abilities. Children spending significant amounts of time in front of screens often struggle with social interactions in offline settings. Should current trends in screen exposure among minors persist, the impact on their development and long-term health

[1] *Teens, screens and mental health: New WHO report indicates need for healthier online habits among adolescents, 25 September 2024, https://www.who.int/europe/news/item/25-09-2024-teens--screens-and-mental-health*

could be profound. Additionally, the problematic use of mobile devices by minors is associated with reduced sleep duration and delayed sleep, likely undermining their overall health and academic performance.

2.2. Institutional Framework (National, EU, International)

Children's rights are enshrined in the 1989 **United Nations Convention on the Rights of the Child (UNCRC)**, to which all EU Member States are signatories. The Convention defines a child as any individual under the age of 18 and stipulates that the best interests of the child must be the paramount consideration in all actions concerning them.

In 2021 the Committee on the Rights of the Child approved General Comment No. 25 (2021) which elaborates on children's rights in the digital environment, building on General comment No. 16 regarding the responsibilities of corporate service providers. Furthermore, at the UN General Assembly in November 2023, a resolution was unanimously adopted to update General Comment No. 25, explicitly detailing the responsibilities of companies providing digital services.

In addition, the EU has fully implemented the Digital Services Act (DSA), which empowers the European Commission (EC) and national authorities to mandate that large online platforms ensure a high level of privacy, security, and protection for children. Focus is placed on safeguarding personal data, regulating personalization mechanisms (profiling), and the prevention of addiction and manipulation through deceptive and ambiguous design patterns (dark patterns). Simultaneously, numerous initiatives and regulatory frameworks are implemented at national, regional, and international levels. A summary of these is provided in **Annex 1**.

The problem remains acute, primarily because insufficient attention has been given to safeguarding the safety of minors during the design stages of digital applications which ideally should discourage addictive behaviors. Furthermore, existing regulatory initiatives have not been fully or effectively implemented.

A small exception is found in legal and regulatory frameworks that mandate the design of applications appropriately tailored to the user's age (Age-Appropriate Design), as already enacted in the United Kingdom, California, and Maryland in the United States, and currently in the final stages of approval in Indonesia. It is worth noting that, **in cases where such detailed and specific regulations have been enforced, many companies significantly adjusted the operation of their services, resulting in measurable positive impacts on children's well-being** (see **Annex 1**: European and International Best Practices).

Therefore, the main question and objective is how the positive international experiences can be leveraged, while simultaneously addressing the transnational nature of this problem. How can Greece promote measures based on Age-Appropriate Design, regionally (EU, Council of Europe) and internationally (OECD, UN)?

3. Strategy Guidelines for the Protection of Minors

3.1. Redesigning Applications without Algorithmic Addiction

It is a moral imperative to redesign the digital world by placing the needs of children at the forefront of digital product and service design, with the aim of preventing addictive behaviours. While there is growing global recognition that children's rights apply equally in both the physical and digital environments—as reflected in the Resolution of the General Assembly of the UN which was established by General Comment 25) - there remains insufficient emphasis on the legal interpretation of children's safety at the design stage of digital products, to address and eliminate addictive behaviours. Moreover, the Digital Service Act (DSA) has come into full effect, mandating that all online platforms ensure a high level of privacy, safety, and digital protection for children. However, its primary focus thus far has been on personal data, profiling, and the prevention of addiction and manipulation through the use of dark patterns.

Children should no longer be left to navigate a world where addictive design strategies – created specifically to capture children's attention – would lead them to excessive engagement to the detriment of their wellbeing and mental health. Strategies employed by many digital platforms to keep users continuously connected, such as infinite scrolling, autoplay

features, and "nudging" techniques, prioritize addiction and dependency over the safety of children. These features, deeply embedded within attention-capturing mechanisms , are intentional and harmful, fostering habits that exploit the cognitive vulnerabilities of children[2].

Nowadays, children are often left to address such challenges on their own, while technology corporations waive responsibility by providing tools like parental control, use statistics and screen time limits. Although such tools may be useful, they transfer the burden on parents that are already overwhelmed, and sometimes onto the children themselves. This is not sustainable or ethical practice. ***Major platforms and digital applications must assume primary responsibility for creating a digital world that is inherently safe for children by design****—even when users are not logged into an account—without shifting the responsibility onto parents, children, or educators*.

Securing Privacy, Safety and Protection by Default: It is imperative to ensure a high level of privacy, safety, and protection for minors as they navigate the digital world. These protections must not be optional; they must be the default standard. Platforms must guarantee that data collection is minimized and that all personal information is fully safeguarded through robust security measures. **The design of digital services should account for the various developmental stages of children, ensuring that platforms recognize the vulnerabilities of minors and mitigate related risks through appropriate design**. This shift in priorities—from addictive mechanisms to protection—is not only necessary but also urgent. We must ensure that the digital world is designed with the sole purpose of delivering genuine, multifaceted benefits to children, rather than capturing their attention, consuming their time, or trapping them in endless engagement. When digital spaces are built with features aimed at maximizing user engagement and exploiting attention, they leave children more vulnerable to both short-term harms (such as mental health issues and exposure to inappropriate content) and long-term consequences (such as addiction and behavioural problems).

Addressing digital asymmetry and digital vulnerability: The phenomenon of digital asymmetry refers to the power imbalance that exists in the digital environment between users and service providers. Complex privacy policies and terms of use make it nearly impossible for users to fully understand their content, forcing consumers to make decisions and offer their consent with limited information. As demonstrated by the Norwegian Consumer Council in an in-depth analysis of the data protection policies of some of the largest platforms, there is lack of meaningful information on how users are actually protected. Relying solely on transparency and consent as tools to protect users, especially minors, has proven to be inadequate. These issues lead to a state of digital vulnerability for users, particularly affecting vulnerable groups such as minors. **Digital vulnerability stems from the power imbalance in the user-provider relationship, driven by factors beyond the consumer's control.** Internal factors include digital illiteracy, information overload, and cognitive biases. External factors may encompass the design of digital environments, choice architecture, the lack of interoperability between services, and the configuration of default settings. Redesigning applications to eliminate algorithmic addiction, combined with appropriate protective measures, preventative strategies, and education, can help mitigate these phenomena. Furthermore, it is essential to establish a duty of care on major service providers, requiring them to protect minors from addictive phenomena and to take the necessary actions to create a digital environment that prevents the conditions for such occurrences.

3.2. Educational Actions and Awareness

The power asymmetry between major technology companies and children who use their platforms is significant. **Companies design state-of-the-art products and services with complex mechanisms for collecting and exploiting personal data that most parents and/or children cannot comprehend.** These companies are adept at exploiting user behaviour for commercial gain, and this imbalance must be addressed. Children are not equipped to navigate

[2] *Summary of Commission Decision of 5 August 2024 relating to a proceeding under Article 71 of Regulation (EU) 2022/2065 (Case DSA.100121 - TikTok Lite Rewards programme) Conclusion (17): 'The Withdrawal Commitment ensures that the provider of TikTok will comply with Articles 34 and 35 of Regulation (EU) 2022/2065, as the withdrawal of the TikTok Lite Rewards programme effectively removes the reward and incentive features of that programme, including the combined use of the Tasks and the multiple attention capture damaging patterns, which directly reward habitual use of, and extended engagement with, TikTok Lite. These rewards and incentive features create, by design, a risk of problematic social media use and behavioural addiction, having actual or foreseeable serious negative consequences for a person's physical or mental well-being, actual or foreseeable negative effects in relation to the protection of minors, and actual or foreseeable negative effects for the exercise of the rights of the child. Being concerned that the TikTok Lite Rewards programme contributes, by design, to this risk of developing problematic social media use and behavioural addiction, the Commission considers this risk cannot be effectively addressed by putting in place additional mitigation measures.' https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52024DSA100121*

environments intentionally designed to manipulate their attention. It is unreasonable to expect them to bear the responsibility for their protection under such manipulative conditions.

This strategy emphasizes the urgent need for platforms to cease basing their profits on carefully engineered, addictive digital environments at the expense of children's well-being. Companies must be held accountable for their persuasive design strategies, which specifically aim to create habitual usage patterns. The digital services most frequently used by children are optimized for revenue generation by capturing and retaining their attention for as long as possible. This strategy calls for a redefinition of priorities i.e. the creation of safe, fair products that prioritize children's wellbeing.

Simultaneously, it is crucial to equip children with tools to navigate the digital world safely and effectively. They must be educated to understand the nature of the digital spaces they visit, including how algorithms function, how to identify manipulative designs, and how to balance their lives between the digital and physical worlds. However, while education is vital, it does not absolve platforms of their broader responsibilities. The burden of ensuring safety must remain firmly with the companies—not with children, parents, or educators.

3.3. Protection Measures and Mechanisms

The strategy for protecting minors from internet addiction requires a multilayer approach that comprises awareness campaigns, new digital protection tools and regulatory interventions. These three categories of measures must operate in a synergistic and complementary manner, as focusing exclusively on a single dimension is insufficient to effectively address the issue. The framework of interventions will evolve simultaneously, combining informational campaigns, actions, and events with concrete projects and a protective regulatory framework that enforces rules on major platforms at both national and European levels. This distinction is crucial for enabling Greece to assume a pioneering role in adopting national regulations and placing a digital strategy on the responsible use of social networks and user protection at the forefront of the priorities of the new composition of the European Commission, with a strong emphasis on safeguarding minors.

Below is a summary of the Awareness, Preventative, and Regulatory measures, along with the specific objectives of the National Strategy.

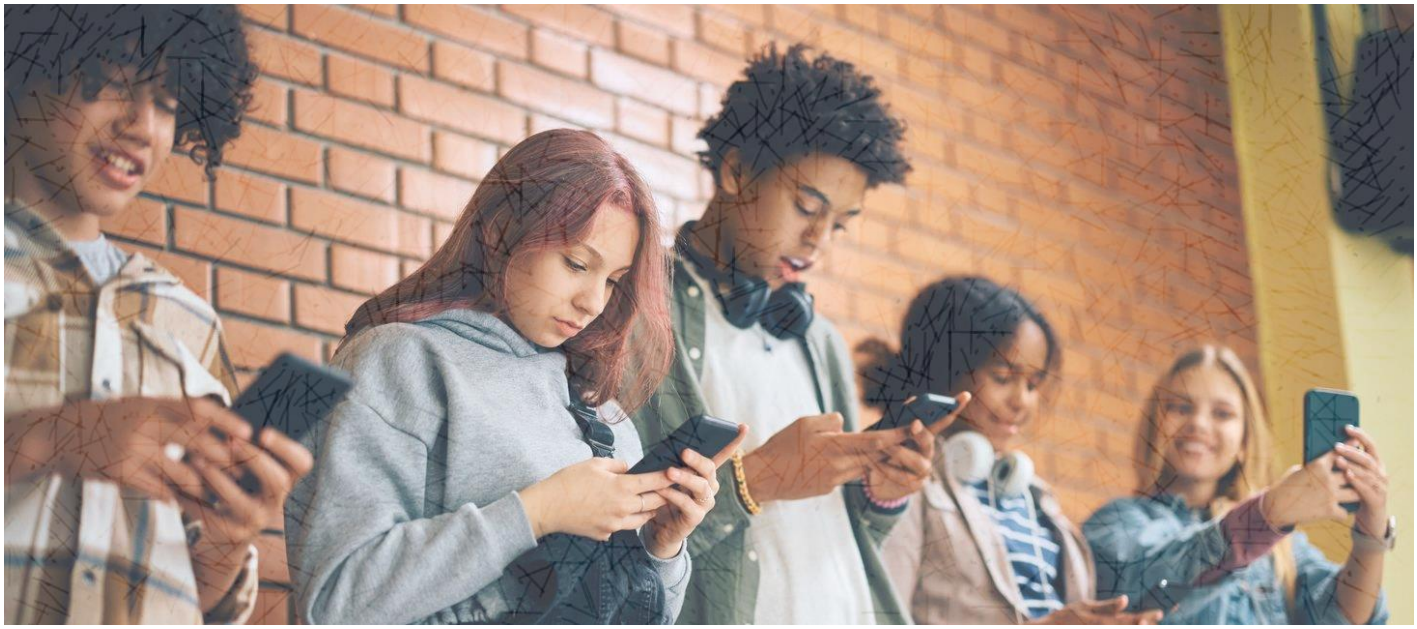
Awareness Measures: Awareness is the cornerstone of the Strategy. These measures aim to inform parents, guardians, children, and the broader public about existing tools to protect minors from addiction, the most significant risks, and the means to address them at both the European and national levels. Simultaneously, best practices will be highlighted, which can be implemented either with or without state intervention, to reduce the use of devices and applications that foster addiction. The target audience includes young parents, minors and the educational community. Key actions:

- ✓ Inform parents and minors about the risks associated with excessive and uncontrolled internet use.
- ✓ Inform parents about available tools and methods to limit uncontrolled internet use.
- ✓ Raise public awareness about the responsibility of major providers/companies to take preventive measures for the content to which they expose their users.
- ✓ Inform the public about their rights concerning data processing and on the content they are exposed to by major providers/companies. .
- ✓ Share insights into the level of internet usage and exposure among young people in Greece and across Europe.

New Preventative Digital Tools: In parallel with awareness campaigns, the government will introduce initiatives that provide parents with easy access to user-friendly tools. Such tools will empower them to protect their children from the excessive use of digital applications, mobile devices, social networks and applications that lead to screen addiction. These measures will include:

- ✓ Tools for reasonable use of the internet by minors
- ✓ Tools for parents for mitigating internet use by minors
- ✓ Training minors on responsible use of the internet

Regulatory Measures: The framework of measures is complete with regulatory interventions that focus on service providers, in contrast to the previous categories that focus on users and parents. The proposed regulatory interventions are part of a national and European strategy. At the national level, it is recommended to adopt international best practices, while at the European level, emphasis is given to proposed actions for better protection of minors and the joint drafting of a new regulatory arrangement, the "Digital Fairness Act", which is part of a long-term mandate of the new European Commission. More specifically, at the **National level** a regulatory framework will be developed to protect minors from mechanisms leading to addiction, while at the same time controlling and monitoring of practices applied by major platforms and digital application providers regarding compliance with national and EU regulations. At the **European level** an EU strategy for the protection of minors from internet addiction will be jointly drafted, with interventions and institutional initiatives, along with joint initiatives with the Commission and Member States.



4. National Strategy – Action Plan

4.1. Implementation Directions - Actions

The European Union was the first in the world to set the framework for the regulation of digital services (see DSA), including the protection of minors. Greece is at the heart of European developments and aspires to make the European legal framework for digital services even more protective in favour of the interest of minors, by fighting the real danger of internet addiction.

Specifically, in the context of implementing this Strategy, Greece supports **the establishment of a pan-European digital age of consent for social media at 15 years**.

With this action Greece aligns with other EU partners who have expressed similar positions, like French President Em. Macron and Danish Prime Minister M. Frederiksen, while also undertaking initiatives to coordinate Heads of States and Governments at the European Council. In this context, Greece is consulting with the European Commission to submit a proposal to amend the Digital Services Act, in view of the coming assessment of the Act by the European Commission in November 2027. Furthermore, Greece supports this initiative at the Council of the European Union through its participating Ministers. Recently, the Minister of Digital Governance, in an intervention at the EU Ministerial Council[3] underlined the need to set out a Europe-wide digital age of consent, in parallel with other actions, interventions, measures and tools discussed.

Additionally, age verification for social media users in Europe can be achieved and implemented through the EU Digital Identity Wallet that would allow cross-border identification of all EU citizens, according to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014, currently in force (Regulation e-IDAS).

Greece is a pioneer in this field, having already implemented the national Digital Identity Wallet (Gov.gr Wallet), also used by Cypriot citizens. An equivalent wallet for minors (Kids Wallet) is underway.

Furthermore, **Greece supports the amendment of the Digital Services Act (DSA) and the development of a new framework under the "Digital Fairness Act," to explicitly prohibit digital mechanisms from platforms and social networks designed** to foster addiction when directed at or used by minors. Beyond the prohibition under Article 28 of the DSA, addressing advertising targeting minors based on user profiling, Greece believes that the design of interfaces and content recommendation systems must be explicitly non-addictive when targeting minors. The current provisions in Articles 25 and 27 of the DSA lack explicit references to the protection of minors and fail to adequately safeguard their well-being.

Additionally, Greece will develop specific proposals for the forthcoming "Digital Fairness Act" through systematic participation in public discussions with the European Commission and Member States, to foresee specialized regulations and measures to protect minors online in relation to their rights as consumers of digital products and applications.

Beyond its contributions to the European regulatory framework, Greece is advancing a series of measures at the national level, which will be implemented through a comprehensive package of informational, preventative, and institutional actions.

4.2. Institutional Initiatives in Greece and the EU

4.2.1. Regulatory Measures in the EU

Greece has prioritised its interventions at the European level, as the European Commission is responsible for ensuring compliance by very large platforms and search engines through specific obligations imposed on them under the DSA, such as risk assessment and mitigation. As noted in the Regulation, addiction in children is one such risk. The EU has already kicked off an official procedure against Meta (16/5/2024) to assess to what extent the company that owns Facebook and Instagram may have violated DSA regarding the protection of minors. Specifically, the EU expresses concern for the fact that Facebook and Instagram systems, including their algorithms, reinforce addiction, drawing the user's attention and

[3] www.mindigital.gr/to be added

causing them to spend time without realizing it or in other words by creating highly addictive behaviour patterns, the so called “rabbit hole effects”. Furthermore, the Commission is also examining the age verification and authentication methods employed by Meta. A similar procedure was initiated for TikTok on February 19, 2024.

Recently (October 2024), the EU sent requests to YouTube and Snapchat regarding their recommendation systems and asked for detailed information on the parameters used by the algorithms to suggest content to users, as well as their role in exacerbating certain systemic risks, including those related to the mental health of users (e.g., addictive behaviour and rabbit hole effects), particularly in minors. Indeed, the European Commission, together with Member States, can exert substantial oversight over very large platforms through a robust, coordinated, and interdisciplinary framework of institutional engagements. These efforts aim to systematically identify risks related to the safety and protection of children and ensure the EU utilizes its institutional authority to monitor platform compliance with their obligations.

Indeed, the European Commission, together with Member States, can exert substantial oversight over very large platforms through a robust, coordinated, and interdisciplinary framework of institutional engagements aiming to anticipate systematic risks related to child safety and protection. This will enable the EU to exercise its institutional authority to ensure platforms comply with their obligations. Within this context, the Greek Administration will pursue the following institutional initiatives to accelerate the drafting and implementation of necessary regulatory measures for effectively protecting minors from internet addiction. While not reiterated in this Strategy, it is emphasized that the internet and digital environments offer numerous, significant, and multifaceted benefits for children. However, the focus here lies on safeguarding minors' rights in the digital world, ensuring the responsible use of their personal data, and addressing mechanisms intentionally designed to foster addiction, which can adversely affect their mental health.

[a] Consultation with Member States and EU for Immediate Adoption of a Europe-wide Digital Age of Consent at 15 years

Greece will prioritize consultations with Member States and the EU to discuss and set a Europe-wide Digital Age of Consent at 15 years. This will include restrictive setting of algorithms for users under 15 years of age, as well as restrictions in social media algorithms for minors. Indicatively, according to such restrictions large platforms will be obliged to:

- ✓ Restrict the promotion of addictive content and reduce exposure to material causing extensive use (e.g. autoplay videos, endless scrolling).
- ✓ Implement mechanisms to manage screen time, such as reminders for breaks and daily usage limits for underage users.
- ✓ Adapt algorithms to protect minors from inappropriate or harmful content, placing priority on education and children-friendly content.
- ✓ Age verification mechanism and parental consent: The proposed regulation would set the "digital age of consent" at 15 years across Europe. Users under 15 would not be permitted to access social media without the explicit consent of at least one legal guardian.
- ✓ Platforms would be required to implement reliable age verification mechanisms to ensure that algorithmic restrictions are applied exclusively to users under 15 years old.
- ✓ The goal is to protect children's mental health and reduce the risks of addiction caused by social media algorithms, thereby providing a safer digital environment for underage users.

[b] Revision of DSA (WG6)

According to Article 91 of the Digital Services Act (DSA), by November 17, 2025, the European Commission will conduct an evaluation and submit a report to the European Parliament, the Council, and the European Economic and Social Committee regarding the implementation of Article 33. This evaluation includes the scope of intermediary service providers covered by the obligations set out in Chapter III, Section 5, of the Regulation. Although this revision focuses on

determining the criteria to classify a platform or search engine as very large, and not on their specific obligations (e.g. assess and restrict systemic risks such as addiction), this process may highlight any failures in addressing systemic risks (such as addiction) by very large platforms, as well as the need to enhance the Regulation with specific obligations for the design and use of systems that by default prevent addiction and ensure protection, safety and health.**[b1] Regulatory initiative to abolish profiling and other relevant mechanisms**

In the context of actions to revise the DSA, or through the regulatory implementation of the current framework or any other useful regulation, a substantial part of the effort will focus on how to incorporate arrangements to abolish automatic user profiling and related mechanisms of recording and exploiting behaviours.

Specifically, article 28 of the Digital Services Act obliges providers of platforms accessible to minors to take appropriate and proportionate measures to ensure a high level of privacy, safety and protection of minors. To implement this obligation, the EU will issue guidelines following consultation with the Council of Digital Services, consisting of coordinators of the 27 Member States. The EU collected views on the matter which must be taken into consideration when drafting the guidelines from 31 July to 30 September 2024. The Ministry of Digital Governance and the General Secretariat of Telecommunications & Post submitted specific views that align with this Strategy (https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14352-Protection-of-minors-guidelines/F3496618_en). These views refer to EU principles and guidelines that should ensure that the internet environment is safe and fair for minors, whereas the digital technology and AI-based algorithms should be designed to prevent children's screen addiction and other negative impact on children's mental health. Moreover, internet technology should limit the use of data and metadata that could potentially harm children's rights, including automatic profiling, reward systems and endless scrolling. The overall analysis of views collected in this context indicated that the issue of digital addiction is also a concern for other agencies, being a factor that undermines safety and protection of minors. This issue is highlighted by the Act also as a potential systemic risk that very large platforms and search engines should mitigate through designing their services to not exploit, purposely or not, the vulnerability and inexperience of minors nor cause addiction. Very large platforms and search engines are also obliged to allow users to access their services without creating a profile.

Therefore, considering that one of the factors that causes addiction in minors is the creation of a profile (as a profile enables the continuous spamming of user with content of their interest), **putting forward an explicit ban on creating profiles for minors (not only for advertisements but for any sort of platform use) is with certainty, a proportionate measure that can be imposed by EU guidelines.**

Based on international best practices, very large platforms and search engines face no technical challenges in implementing this measure, as it is directly related to their existing obligations. Platforms that already implement profiling restrictions for advertisements should extend these measures to cover all services accessed by minors. Therefore, a general prohibition on profiling for minors is a proportionate measure that can help combat addiction. Beyond the comprehensive ban on profiling for all minors—which, as explained, entails no significant technical difficulties in implementation —additional changes to platform design are required to prevent addiction. Some examples are time limits for minors set by platforms, banning autoplay, restrictions in endless scrolling, banning nudging. Such measures can contribute to addiction restriction and, since they require no special technical implementation, are also considered proportionate and therefore in the context of article 28 provisions.

All the above, further to being discussed in the Commission, will be set forward by the Ministry of Digital Governance and the Hellenic Telecommunications and Post Commission (as a member of the Digital Services Council) in all relevant forums, such as the DSA Council or relevant working groups, to shape the guidelines respectively. **[b2] Announcement of the Greek proposal for the Charter of Digital Rights of Children and European Commission consultation to draft a Pan-European Charter**

In the context of actions to revise DSA, and/or through the regulatory implementation of the current framework or any other suitable regulatory procedure, actions will be taken to draft and adopt a Charter of Digital Rights of Minors in the EU. Greece may indeed play a leading role in this EU-level consultation on establishing new rights for the protection of minors. Greece will announce its own proposal on a charter of digital rights that will set the legislative directions for the EU to follow, putting the protection of minors at the heart of these initiatives. The charter of digital rights will refer to the

risks and challenges from uncontrolled use of the internet, to the opportunities and the potential for a common European digital policy for responsible internet use, for recording and acknowledging new rights for minors in the digital world.

Some of those rights would be:

- ✓ Right not to be tracked
- ✓ Right to meaningful personalisation
- ✓ Right to fairness by design
- ✓ Right to know one's digital alter ego

[c] Setting up a task force to draft the "Digital Fairness Act" and amend the "Digital Services Act".

A task force will be set up to implement the above institutional interventions regarding DSA revision and draft positions for the coming "Digital Fairness Act". The task force will have the following duties:

- ✓ Monitor developments and the preparatory procedure for the "Digital Fairness Act"
- ✓ Collect content and proposals from think tanks to form the framework
- ✓ Liaise with European Commission and Eurogroup representatives to draft the proposals
- ✓ Form a framework of legislative proposals (or proposed legislations?) at the EU level
- ✓ Draft proposals to amend the "Digital Services Act" based on past interventions

Indicatively, some of the legislative arrangements this task force will examine: (i) Definition of "tracking". There is no legal definition of this term as something broader than profiling. (ii) "Profiling" is defined in para. 4 article 4 of the General Regulation of Data Protection"; DSA prohibits advertisements based on the profile of minors, as well as on profiles that use special categories of personal data according to GDPR. Nevertheless, those provisions may be insufficient to address the problem and the negative impact of advertisements, as well as the need for a stricter protection of minors, given that the provisions i) only apply to internet platforms (e.g. this does not cover a newspaper site or a regular business store site) and ii) do not cover all forms of advertisements, nor address the main issue, i.e. the negative impact of data exploitation and of non-transparent algorithm systems.

[d] Non-binding regulatory measures.

Proposal for a resolution to address internet addiction: a European Parliament resolution is proposed to identify the risks minors face from extensive and uncontrolled internet use. The resolution will be drafted jointly with the group of Greek MPs in the European Parliament and will:

- ✓ Recognize or Acknowledge the risk minors face from excessive and uncontrolled internet use
- ✓ Highlight the existing regulatory gap in addressing events that cause addiction (doom scrolling, profiling, dark patterns etc.) and the lack of appropriate enforcement mechanisms
- ✓ Recognize or Acknowledge the need for a horizontal provision for a EU-wide social media age restriction
- ✓ Identify a number of rights in the digital world (right not to be tracked, right to meaningful personalisation, right to fairness by design, right to know one's digital alter ego) and define their content.

4.2.2. National Regulatory Measures

Greece will also prioritize institutional interventions at the national level, independently of the actions and initiatives outlined above at the European level. Should the implementation timelines for some of these measures coincide, the alignment of the proposed national regulatory interventions will be considered.

[a] Setting of the Digital Age of Consent at 15 years and regulations for age verification mechanisms.

This intervention aims at drafting legal rules abiding by the principles of good legislation to set the Digital Age of Consent at 15 years. Major platforms and social networking applications will be required to verify the age of their users with documented evidence and not rely solely on a simple "self-declaration" of age. This law addresses the need for increased parental oversight and control over minors' use of social media to protect them from risks such as exposure to inappropriate content, screen addiction, cyberbullying, and privacy violations. The main guidelines of this legislative initiative are:

- ✓ Age limit at 15 and parental consent: this provision will set the “digital age of consent” at 15 years. Users under the age of 15 will not be allowed to use intermediary internet services and especially social networking, without an explicit consent of at least one person who is legal guardian. Above the age of 15, minors will be able to use social media with advisory parental monitoring.
- ✓ Age verification: intermediary internet service providers, especially social media providers, will be obliged to check user age. Note that a simple “statement” of age or of date of birth will not suffice, and providers will be obliged to use additional age verification means such as the use of public documents.
- ✓ This proposal complies with the GDPR that allows member states to set the age of digital consent between 13 and 16 years. In Greece the age of consent is 15 years. The same approach will be followed for the digital age of maturity.
- ✓ Social media platforms will have to implement age verification mechanisms and ensure parental consent for users under the age of 15. Non-compliance will result in fines and penalties imposed by the relevant Greek regulatory authorities.

[b] Setting a Parental Control Mechanism on digital devices.

The objective of this intervention is the legislative preparation for the establishment of a mandatory parental control mechanism on devices for displaying digital content. The regulation will require manufacturers of devices designed for internet access and sold commercially in the Greek market (e.g., smartphones, tablets, computers, gaming consoles) to pre-install or provide easy access to parental control software. Such software will allow parents to:

- ✓ Regulate screen time
- ✓ Block inappropriate content
- ✓ Monitor device usage

The parental control software must be easy to set up, requiring no specialized technical knowledge. Additionally, its implementation will comply with the General Data Protection Regulation (GDPR), ensuring the protection of users' privacy.

5. Information and Preventive Actions and Projects

5.1. Systematic mapping of internet use and minors ’behaviour in Greece

An interdisciplinary scientific task force will carry out nation-wide detailed research to collect data on the use of internet in Greece, the behaviour of minors, the status, potential trends, and the impact of interventions as they are gradually implemented. The research results will be published on an informational website managed by the Ministry of Digital Governance, which will provide updates on all relevant topics and information regarding protection from internet addiction. Additionally, the results will help to dynamically shape the policies and interventions outlined in this Sstrategy.

5.2. Public awareness actions

[a] Information website on installing reasonable usage mechanisms - parco.gov.gr

parco.gov.gr is a new website launched by the Greek government to support parents and guardians in ensuring the safety of children and teenagers on the internet and social media platforms. The name "Parco" is derived from the term "parental control" and focuses on educating and informing on the use of tools for parental control.

✓ **Parental control guidelines** for devices (iOS, Android).

✓ Limiting online time

✓ Blocking inappropriate content or websites

✓ Monitoring the content children have access to

✓ Tracking the device's location.

[b] Part 1. Awareness campaign – Internet addiction risks and responsible internet usage

The first part of the campaign focuses on the risks posed by internet addiction and excessive use of the internet. Based on the initial findings of the previous initiative, a comparison of addiction levels in Greece versus the rest of Europe and globally will be presented. Examples of young individuals affected by uncontrolled internet use will be highlighted, along with recommendations for fostering responsible internet usage. Proposed actions include:

✓ Television campaign: TV spots with related content

✓ Social Media campaign: Utilizing social media to promote responsible and reasonable use. Responsible use does not mean non-use. Engaging influencers to effectively convey the message against internet addiction.

[b] Part 2. – User rights, parental power, providers' responsibilities

The second part of our awareness campaign focuses on the responsibilities of major providers toward their users and the rights users hold. The goal is to counter the phenomenon of digital asymmetry by providing the public with essential information about the manipulative tactics used by major platforms/providers to create addictive patterns and retain users' attention, often through inappropriate means. Users have a comprehensive? set of rights, and it is crucial to inform them about these. This campaign will also educate parents about the tools available for limiting their children's internet usage, including existing built-in mechanisms within applications and consoles.

5.2.1. School Campaign - "A Day to Surf in the Digital World"

A school-based campaign will be launched to inform students about the dangers of internet addiction, the responsibilities of major providers toward them, and the rights they hold in relation to major platforms.

The campaign could be kicked-off with the designation of a specific day (e.g., The Three Hierarchs) as a national "Digital Navigation Day" or "Digital Learning Day." On this day, schools across the country would engage in thematic activities each year, focusing on the use of new technologies, their benefits, and the potential impact on mental health. The day would be dedicated to promoting responsible technology use and addressing addiction. Each year's theme could be chosen by the Ministry of Education and the Ministry of Digital Governance, ensuring a fresh and relevant focus on digital literacy and well-being.

5.2.2. Implementation of a Digital Citizen application for minors - Kids Wallet:

The Kids Wallet application aims to create a safe and educational environment for children. It will connect to parents' Gov.gr/ Wallet enabling parental control and providing support to all their digital activities. Some of the main functions will be:

Identity and Digital Documents: Kids Wallet will have a digital identity of the child and additional documents such as school identities, health records and information on participation in activities.

Safety provisions and activity reports: parents can define the parameters of how their children use the application, such as use during school times or internet access, and will receive reports for various activities such as addition of documents, id verification or use at events.

Protection and use restrictions: the Parental Control feature within the Wallet will ensure that it cannot be uninstalled without parental consent. It will also offer the ability to block the phone during school hours. Parents can select restricted functionalities for specific time periods, using pre-configured setting packages, such as for school hours or bedtime, tailored to the child's age.

6. Funding (National Schemes and Financial Footprint)

Actions will be funded in cooperation with the Ministry of Finance utilising financing mechanisms such as the Public Investment Programme, which covers stand-alone national projects and joint EU projects funded by EU resources (such as the NSRF).

7. Road Map for Action Plan Implementation

7.1. Road Map and Milestones

Below follows a brief presentation of measures, actions and stages of the Action Plan, with milestones for its successful implementation:

Measures		**Actions and Projects of Information and Prevention**	
EU	**Greece**	**Awareness Actions**	**New tools and prevention**
Establish the Digital Consent Age at 15 Years **Revise** the DSA **Draft** a Charter of Digital Rights of Minors **Prepare** the "Digital Fairness Act"	**Establish** the Digital Consent Age at 15 Years. **Establish** a Mechanism of Parental Control in Digital Devices	**Actions** toward raising public awareness **Campaign** in schools - "Digital Navigation Day"	Systematic **recording** of internet use and behaviour of minors in Greece **Implementation of Kids Wallet** a Digital Citizen application for minors -

Milestones

[M1] Nationwide Study on Internet Usage and Behaviour of Minors

The study will be conducted nationwide to collect data on internet usage, minors' behaviour, the current state, and potential trends. The findings will be published on a website managed by the Ministry of Digital Governance, offering resources for children and parents. The website, **parco.gov.gr**, is already operational and includes information on available internet usage restriction tools and the risks of addiction.

[M2] Interdisciplinary Working Group for Monitoring, Preparation, and Interventions on the "DSA" and "DFA"

The working group will develop a framework of proposals for the Greek government to contribute to the formulation of the "Digital Fairness Act" and the upcoming amendment of the "DSA," emphasizing the protection of minors from internet addiction.

[M3] Creation and Publication of a Digital Rights Charter for Internet Users

The Digital Rights Charter will represent the first step in promoting the national strategy at the European level. This position paper will recognize a series of digital rights and outline Greece's direction in protecting minors in the digital environment.

[M4] Public Awareness Campaign (Parts 1 and 2)

The campaign aims to inform the public about users' rights against major platforms, the platforms' obligations, the risks of uncontrolled internet use, and the measures being implemented by the Greek government.

[M5] School Awareness Campaign and Digital Navigation Day

In collaboration with the Ministry of Education, a targeted campaign will inform students, teachers, and professors about the dangers of internet addiction and responsible use. Additionally, a "Digital Navigation Day" may be established to familiarize students with new technologies, opportunities, and risks.

[M6] Launch of KidsWallet

A digital citizen application for minors (KidsWallet) will be launched, providing appropriate tools to ensure responsible internet use, while enabling parents and guardians to play a more active role in their children's digital experiences.

[M7] National Institutional Interventions

Following the example of countries like France, Greece will introduce national legislative initiatives as part of its framework of measures. These will aim to ensure responsible internet use and act pressure on major platforms and the EU to adopt more effective rules for protecting minors.

[M8] Resolution Proposal with Greek Members of the European Parliament

Building on the "Digital Rights Charter," the working group, in collaboration with the Greek delegation to the European Parliament, will draft a resolution calling for initiatives to address addiction and the recognition of new digital rights by the European Parliament.

[M9] Interventions on the DFA and DSA

The working group will submit proposals for the formulation of the "Digital Fairness Act" and amendments to the "Digital Services Act," alongside institutional interventions and the results of consultations with the European Commission and other Member States.

[M10] Second Phase of Public Awareness Campaign

This phase will inform the public about the outcomes and best practices for responsible and reasonable internet use.

[M11] Nationwide Study to Assess changes in Internet Usage and Behaviour

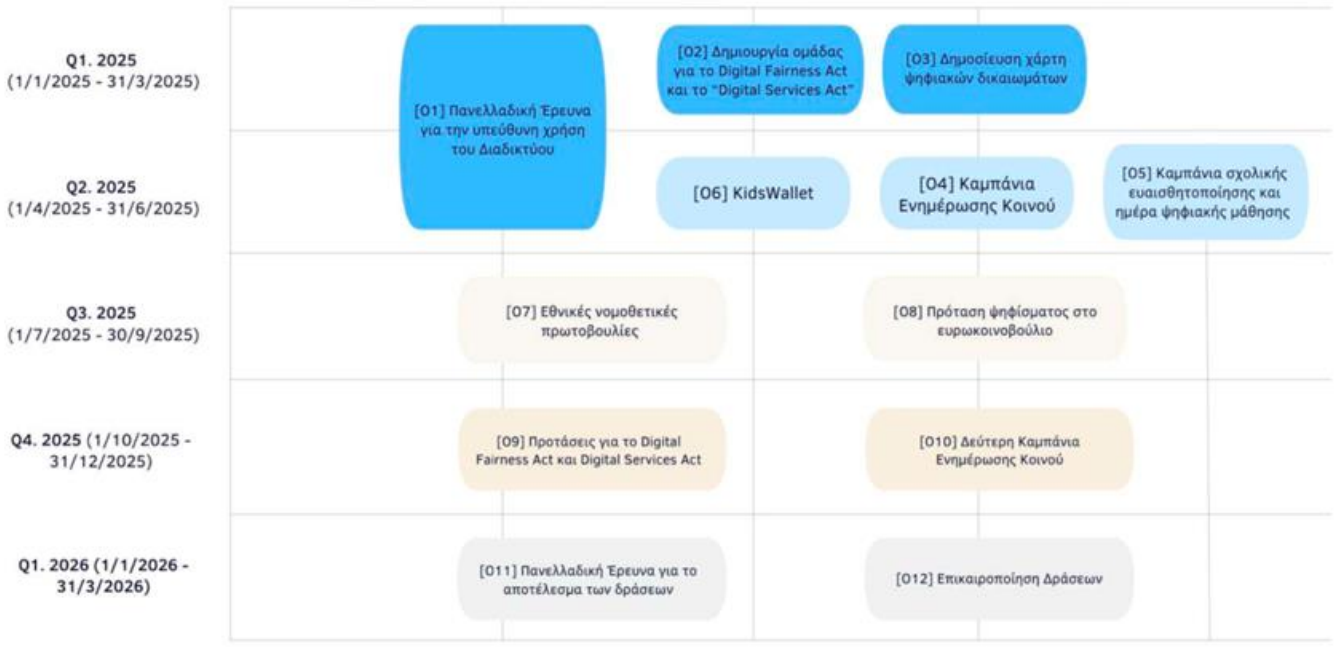
A nationwide study will be conducted to evaluate any changesin internet usage and behaviour among minors, assessing the impact of the measures and actions implemented during the first year of the Strategy.

[M12] Update of Strategic Actions Based on Post Evaluations

The actions of the strategy will be updated based on the evaluations and the overall impact of the action plan.

7.2. Action Plan Timeline

The proposed timeline for completing the strategy and achieving the 10 milestones extends over a period of **12-18 months**. Some initiatives are directly linked to developments at the European level, and adjustments to the timeline may be necessary as circumstances evolve. A goal of the strategy is to align the actions which are proposed at the European level such that they coincide with the initiation of procedures for the formulation of the **"Digital Fairness Act",** ensuring coherence and synergy between national and European efforts.



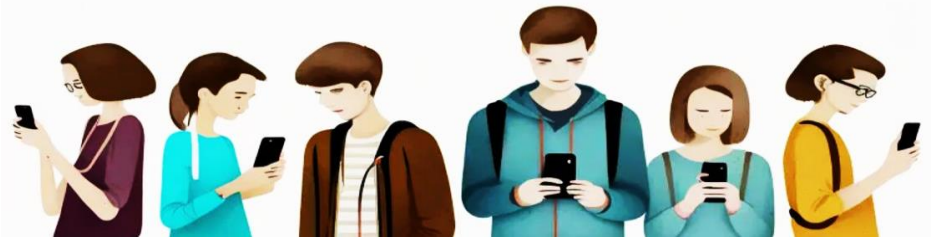
8. Strategic Communication Plan

A comprehensive Communication Plan will be implemented to ensure transparency, collaboration, and the active participation of all stakeholders involved in the National Strategy. The objectives include public awareness, building trust, and fostering the engagement of citizens and organizations. The plan targets various groups, such as the general public, students, parent-teacher associations, scientific bodies, and the media, using clear, consistent, and tailored messages. Communication channels include digital media, traditional media, public events and audiovisual material. Effectiveness will be assessed through qualitative and quantitative data for ongoing improvement of impact. The main objective is to ensure support and adoption of strategy-related actions and facilitate their successful implementation.

9. Action Plan monitoring procedure

To implement the National Strategy, working groups will be established comprising officials and experts from the Ministry of Digital Governance, the Ministry of Health, the Ministry of Education, the Special Secretariat for Long-Term Planning, and the General Secretariat for Legal and Parliamentary Affairs.

The supervision, assessment and updating of the Strategy will be a dynamic and ongoing procedure that will ensure effective and dynamic adaptation of actions. Supervision will include systematic monitoring of actions' progress, whereas assessment will focus on impact analysis, effectiveness analysis and compliance of actions to initial goals. Updating will be necessary to ensure that Strategy and actions remain relevant and realistic, and will consider new challenges, technological and regulatory developments or policy priorities. The goal is for the Strategy to remain in line with the needs of society and national goals.



10. ANNEX

10.1. International legal framework for children's rights in the digital environment

Children's rights are included in the Convention on the Rights of the Child of the UN, 1989 (UNCRC), which was adopted under Resolution 44/25 and was ratified by all EU Member States. For the purposes of the Convention, a child means every human being below the age of eighteen years, and in all actions concerning children, the best interests of the child shall be a primary consideration.

In 2021 the Committee on the Rights of the Child approved General Comment No. 25 (2021) on children's rights in relation to the digital environment, and also included a reference to the responsibilities of businesses for the respect of the rights of children in the digital environment, on the basis of General comment No. 16 on State obligations regarding the impact of the business sector on children's rights. Moreover, it is increasingly acknowledged that children's rights apply both in the physical and the digital worlds, as reflected in the Resolution of UN's General Assembly for the Rights of Children in the Digital Environment of 2023.

Furthermore, this international framework for the protection of children in the digital environment is enhanced by the guidelines of the Council of Europe (2018), the Council of Europe Strategy for the Rights of the Child (2022-2027), which refers to the safe use for technologies for all children, the Guidelines of the International Telecommunication Union (ITU) of 2020 (child online protection guidelines), Resolution 67 of 2022 that describes the role of ITU-D (Development Sector) for the online protection of children (COP - Child Online Protection), Resolution 179 of 2022 on the general role of ITU for the child online protection (COP), and OECD recommendation of 2021 on children in the digital environment.

10.2. EU framework on children's rights in the digital environment

Children protection and children rights promotion are a major goal of the EU, as established in article 3 of the Convention for the European Union, the European Convention on Human Rights (1950) and the Charter of Fundamental Rights of the European Union, (2012, article 24). Moreover, the EU has set as priority the implementation of children's rights in the digital environment.

The legal framework and the policy framework of the EU is constantly developing with the objective of ensuring the safety of children online in an effective way. A strong EU legislation aims at implementing children's rights in the digital environment. Indicatively:

- ✓ Artificial Intelligence Act - Regulation (EU) 2024/1689 prohibits systems that exploit any of the vulnerabilities of a natural person due to their age (article 5) and requires that high risk systems consider any potential negative impact on children (article 9).
- ✓ Regulation (EU) 2024/1183 on European Digital Identity (EUDI) sets the framework for setting an integrated, reliable and safe digital wallet / digital identity.
- ✓ Regulation (EU) 2022/2065 – Digital Services Act provides for special protection for minors (article 28).
- ✓ Regulation (EE) 2023/988 on general product safety acknowledges the health risks involved in digital products, especially for children.
- ✓ Regulation (EU) 2023/2854 - Data Act establishes a uniform framework that determines who has the right to use product data or similar service data, under what conditions and on which basis. There is no explicit reference to minors, only to the use of dark patterns.
- ✓ General Regulation (EU) 2016/679 on Data Protection (GRDP) provides for additional protection for children's data.
- ✓ Directive 2010/13/EU concerning the provision of audiovisual services prohibits the processing of personal data of minors for commercial purposes and requires that video platforms take appropriate measures for the protection of minors (articles 6a and 28b).
- ✓ The proposed CSAM/CSAR (Child Sexual Abuse Material/Child Sexual Abuse Regulation) also strongly provides for prevention and safety by default.

The EU has issued strategic documents for children's protection and for further protection of children's online rights.

In this context, with the EU Strategy for children's rights 2021-2024, as approved in March 2021, the EU aims also to secure children's rights in the digital environment while it acknowledged that excessive screen and online exposure is of concern for the health and mental wellbeing of children, as it leads to increased anxiety, poor attention, poor vision and lack of physical activity.

The EU asked ICT companies to:

- ✓ Ensure that children's rights are included in digital products and services - already at the design stage and by default,
- ✓ Provide children and parents with the necessary tools to monitor screen time and behaviour, protect them from the results of excessive use and addiction to internet products, and
- ✓ Enhance measures for addressing harmful content and inappropriate commercial communication, like through easy-to-use reference and block channels or effective age verification tools.

In 2022 the New European Strategy for a better internet for kids (BIK+), aimed at securing that all children are protected, empowered and respected online, with a special emphasis on age-appropriate digital services. In the context of the need for a new strategy emphasis was put also on the issue of harmful internet, including exposure of children to addictive behaviours and related risks when designing online interfaces that (purposely or not) exploit children's lack of experience and may result in addictive behaviour. If was also explicitly noted that despite EU legislation (Directive for audiovisual media services and GDPR?) age verification mechanisms and parental consent tools are still ineffective in many instances.

In 2023 the European Declaration on Digital Rights and Principles for the digital decade focused on the protection and empowerment of children and young people in the digital environment, with the objective of promoting positive experiences for children in an appropriate and safe digital environment for their age. It also focused on protecting all children from illegal monitoring and profiling, especially for commercial purposes.

The European Parliament has also issued some reports and resolutions for further protection of children's rights in the digital world.

The Resolution of the European Parliament of 17 January 2024 on virtual worlds makes reference to the fact that special attention should be paid on addictive and misleading design of digital services, and it also alerts about the potential health issues that may occur from the interaction with virtual worlds, such as addiction. The Resolution also underlines that it is important for online services and products used mainly by children to be safe for children already by design and by default. It also clearly stated that special attention should be given to the addictive and misleading design in digital environments and the special vulnerability of minors and young people that may occur from the interaction with virtual worlds was underlined.

The Resolution of the European Parliament of 12 December 2023 on the addictive design of internet services highlights the serious impact of addictive design on everybody, but especially on children and adolescents. It underlines the need for further research regarding addictive design, its forms and impact, and asks the Commission to coordinate, facilitate and fund a targeted research. The Resolution also invites the Commission to put additional efforts internationally to promote the regulation of addictive internet design; it highlights the need to promote and implement initiatives for policies and industrial models for safety, from the stage of design of digital services and products for children, which can encourage compliance with children's rights. The issue of addictive design not being fully covered by current EU law was also clearly put forward; if not addressed, this could result to further downgrading of the health of minors.

The Resolution of the European Parliament of 18 January 2023 on the protection of consumers in internet games, which puts emphasis on by default design that leads to addictive behaviour. Scientific research has shown that during puberty and adolescence individuals are more vulnerable and this results in excessive online gaming time, which is worsened by the manipulative design and can lead to addiction.

The Resolution of the European Parliament of 3 March 2022 on AI in the digital era underlines that AI systems that interact with children or affect children in any way must take into account children's rights and vulnerabilities. Such systems should meet the highest standards available for safety, protection and privacy by design and by default.

Finally, European standardisation organisations CEN και CENELEC adopted an Agreement on age-appropriate design of digital services in 2023, setting a clear procedure for digital service providers to be followed when designing products and services available to children.

10.2.1. DSA and protection of minors in EU and Greece

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and on amending Directive 2000/31/EC (Digital Services Act - DSA) considers necessary a "responsible and diligent behaviour by providers of intermediary services is essential for a safe, predictable and trustworthy online environment and for allowing Union citizens and other persons to exercise their fundamental rights" (point 3). The protection of minors is an important policy objective of the Union (point 71) and in this context the Digital Services Act ensures better protection for minors with special legislative provisions (article 28) and obliges online platforms to respect their fundamental rights when they are on the internet.

Specifically, further to general rules introduced by the Digital Services Act for all online platform providers, such as prohibition of dark patterns (article 25), implementation of terms and conditions with a diligent, objective and proportionate manner and specifically explanation of terms and any restrictions concerning the use of the service in a way that minors can understand (article 14), provisions against illegal activity and illegal content (articles 9, 16, 18, 22 and 23) and high transparency requirements (articles 15, 24, 26 and 27), these measures are complemented mainly on the basis of article 28 of the DSA and the obligation borne by providers of online platforms used by minors to "take appropriate and proportionate measures to protect minors… with the highest level of privacy, safety and security for minors" with a special emphasis on the fact that "providers of online platforms should not present advertisements based on profiling 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" (point 71).

In addition, very large online platforms and very large online search engines with a monthly average number of users equal to or over 45 million in the EU (e.g. Instagram, TikTok) have additional obligations to Assess (article 34) and Mitigate (article 35) systemic risks arising from the design or operation of their services and systems (including algorithmic systems) or from the use of their services. Also, very large platforms and search engines are obliged to provide at least one option for each recommender system they use which is not based on profiling (article 38).

Digital Services Act acknowledges that the way companies design their services is generally optimised to benefit their, often advertising-driven, business models and can cause societal concerns (point 79).

One of the four categories of systemic risks acknowledged by DSA concerns the actual or foreseeable impact of digital services on the exercise of fundamental rights, as protected by the Charter, including children's rights. Such risks may arise, for example, in relation to the design of the algorithmic systems. When assessing risks to the rights of the child, providers of very large online platforms and of very large online search engines should consider for example how easy it is for minors to understand the design and functioning of the service, as well as how minors can be exposed through their service to content that may impair minors' health, physical, mental and moral development. Such risks may arise, for example, in relation to the design of online interfaces which intentionally or unintentionally exploit the weaknesses and inexperience of minors or which may cause addictive behaviour (point 81).

Another category of risks stems from similar concerns relating to the design, functioning or use, including through manipulation, of very large online platforms and of very large online search engines with an actual or foreseeable negative effect on the protection of public health, minors and serious negative consequences to a person's physical and mental well-being. Such risks may also stem from online interface design that may stimulate behavioural addictions of recipients of the service (point 83 and article 34).

Providers of very large online platforms and of very large online search engines should take into account the best interests of minors in services design (point 89).

Further to the above, DSA (article 44) supports the configuration and implementation of standards with measures targeted to protect minors online.

Measures that refer on the protection of minors are the following:

✓ Principle of the "best interests of the child"

✓ The right to children's protection

✓ The right to free expression

✓ The right to avoid discrimination

✓ The right of protection of personal data

According to the Digital Services Act platforms used by minors are prohibited to have targeted advertisements based on profiling or use of personal information.

Also, children must be protected from online risks such as harassment, bullying, false information, illegal content and/or individuals lying about their identity.

Greece harmonized its national legislation with the Digital Services Act with Law 5099/2024 (Α΄ 48) "Measures for implementing Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) and other provisions"

The role of the "National Coordinator of Digital Services" in the context of the Digital Services Act was assigned with Law 5099/2024 (Α΄ 48) to the Hellenic Communications and Post Committee (EETT), the main competence being the supervision of compliance of digital services providers stationed in Greece. The EETT is also in charge of managing user complaints (private users and companies alike) for violations of the Act, collection of information from providers regarding the observance of the Act, imposing penalties/fines, coordination in Greece and cooperation with other authorities for the implementation of the Act and cooperation with Regulators of other Member States and the European Commission.

Further to the National Coordinator, Law 5099/2024 (Α΄ 48) appoints the following two (2) competent authorities, in charge of supervising providers and imposing specific provisions of Act (Competent Authorities):

✓ The National Council for Radio and Television (NCRTV), which monitors the observance of providers' obligations regarding advertisements on internet platforms (article 26, para. 1, a-c and para. 2) and takes measures to protect minors (article 28 para. 1).

✓ The Hellenic Data Protection Authority that monitors the observance of providers' obligations regarding the provision of information to users about how advertisements appear and are targeted (article 26, para. 1, d and para. 3), as well as protection of minors' personal data (article 28).

10.2.2. AI ACT

The Artificial Intelligence Act (AI Act) introduces a comprehensive regulatory framework to govern artificial intelligence (AI) within the European Union, categorizing AI systems based on their risk levels. This Act represents a significant step toward ensuring the responsible development and use of AI, particularly in safeguarding children, who are explicitly recognized as a vulnerable group requiring special protection (point 28).

One of the primary objectives of the AI Act is the protection of children from specific vulnerabilities they face in the digital environment. A key provision is the outright prohibition of AI systems that exploit vulnerabilities due to age, including children (Article 5). This includes AI systems or applications that manipulate human behaviour to override users' free will, such as manipulative games or applications designed to use voice assistance to encourage dangerous behaviours in minors. Additionally, the Act mandates strict risk assessments for high-risk AI systems and classifies AI systems used in educational settings as high-risk, requiring stringent management and oversight (Articles 6 & 7, Annex III). This prioritizes the protection of children's rights and safety. Furthermore, the Act enforces transparency for AI-generated content, such as chatbots and deep fakes, requiring clear disclosure to users that they are interacting with a machine. This ensures that users, particularly minors, are informed of the artificial nature of the content they engage with (points 133 and 134).

The AI Act is currently in a transitional phase, marking the beginning of a complex implementation process. The effective application of the Act's provisions, through clear and strict guidelines—especially those concerning child protection—and continuous monitoring via established compliance mechanisms, is crucial to safeguarding the rights of minors in the digital age.

10.2.3. DIGITAL FAIRNESS ACT

On 3 October the European Commission announced the results of the "Digital Fairness Check", an assessment about whether current consumer protection rules are adapted to changing internet practices. The report spotted a number of unfair practices, like "dark patterns", addictive interfaces and complex procedures to annul inscriptions that may lead to drafting the future Digital Fairness Act (DFA). The new European Commissioner will propose a text for Democracy, Justice and Rule of Law that aims at overall enhancing consumer rights while adding another level to the already dense regulation field. New regulations are a unique opportunity for businesses in the EU and beyond to show their dedication to practices focusing on the user.

In 2022, the European Commission initiated a public consultation known as the Fitness Check to evaluate the effectiveness of existing regulations under the Digital Services Act (DSA) in protecting online consumers. The Fitness Check specifically examined the effectiveness of three key EU directives: the Unfair Commercial Practices Directive, the Consumer Rights Directive, and the Unfair Contract Terms Directive. On October 3, the Commission published its much-anticipated report.

The report focused mainly on deceptive, manipulative and addictive practices, known as "dark patterns" – unfair practices in the design of digital interfaces that make consumers take decisions they would not take otherwise. The impact of such practices, which is enhanced by individualisation based on behavioural data, challenges the protection of online consumers.

Although such practices are not new, their dissemination and effectiveness have increased, raising concerns particularly in the US, the UK and South Korea. In Europe, a large number of legal documents are applicable to these dark patterns, addressing them not only as unfair practices but also as a breach of law on the protection of personal data and the prohibition of abuse of dominant position. Considering the substantial damage risks, the Commission deemed necessary to ban them more explicitly through the DSA.

The recent report underlines the main damages related to dark patterns: loss of autonomy and privacy, cognitive overload, mental damage and reduced collective wellbeing through negative impacts on competition and price transparency. It is important that the Commission estimates the cost of online deception for consumers to € 7 bn in 2023. This compares to a cost of compliance for businesses estimated between € 511 m and € 737 m – a strong argument in favour of the regulation.

Following this assessment, the mission letter of Ursula von der Leyen to Michael McGrath, the Commissioner responsible for democracy, justice, and the rule of law, which was made public last September, determined the priority strategies to enhance customer protection and promote democratic integrity in the EU. In this letter, President Ursula von der Leyen refers to the need to draft a future Digital Fairness Act, "to tackle unethical techniques and commercial practices related to dark patterns, marketing by social media influencers, the addictive design of digital products and online profiling, especially when consumer vulnerabilities are exploited for commercial purposes"

At the hearing before the European Parliament on 5 November 2024, Michael McGrath presented his vision of the future Digital Fairness Act. At his opening statement McGrath underlined the need to enhance customer rights in the digital market. The DFA aims to address addictive design in digital products, focusing on practices such as features that look like games of chance, and loot boxes often found in video games. Such features have raised concerns because of their ability to exploit children's vulnerabilities and encourage excessive spending. The DFA aims to mitigate such risks by implementing regulations that protect minors from such manipulative design techniques. In response to concerns expressed by several members of the European Parliament, he mentioned that the DFA will be drafted to bridge the gaps of existing law and not duplicate existing provisions.

One of the key pillars of the DFA is the protection of minors from harmful online practices. Responding to questions about safeguarding minors, Michael McGrath emphasized the unique challenges they face. The DFA presents an opportunity to introduce an additional layer of accountability for platforms, potentially requiring them to consider user vulnerabilities when designing their interfaces. This could involve risk assessments or even the introduction of new subjective rights for minors or their parents, such as a right to customization that enables users—or parents of minors—to directly influence choice architecture.

Recognizing children's unique sensitivities to persuasive digital strategies, the DFA represents a significant step toward protecting young users beyond their physical presence on online platforms. It addresses fundamental issues concerning

how children interact with and are influenced by digital environments, ensuring their rights and well-being are central to the digital marketplace.

As part of these efforts, Commissioner McGrath announced an upcoming study focusing on the behavioral impacts of marketing techniques in online games targeted at children. This study aims to provide empirical data on how these marketing strategies affect young users, contributing to future policy decisions. The findings are expected to be presented next year, offering a more comprehensive understanding of the challenges children face in digital spaces and guiding the development of more effective protection measures.

10.2.4. ITU

The International Telecommunication Union (ITU) is the specialized United Nations agency for telecommunications and Information and Communication Technologies (ICT). Our country has been a member of the organization since its establishment in 1865. Today, the ITU serves as a framework within which governments and the private sector come together and collaborate to develop networks and telecommunications on a global scale. The ITU's engagement with child protection online began with the Joint Coordination Activity on Child Online Protection (JCA-COP), established in 2012 by the ITU-T Study Group 17: Security. Since 2015, a permanent committee of the ITU Council on Child Online Protection (CWG-COP) has been operational. The CWG-COP has identified appropriate actions for child protection online, including raising awareness on child safety issues and supporting Member States in developing roadmaps related to the COP initiative. This Council committee is open to participation by all stakeholders and serves as a platform for ITU members to exchange views, draft best practices, and foster cooperation at national and international levels.In its meeting on October 1, 2024, the CWG-COP decided to organize a meeting between the ITU and companies providing social media platforms. The ITU-D, specifically Study Group 2: Digital Transformation, was appointed to lead this initiative.

Although the ITU was the first standardization organization to address child protection online, it has not yet made significant progress in drafting legislative documents, as the two referenced resolutions (Resolutions 67 and 179) remain the only ones issued. Specifically, regarding the issue of protecting children from internet addiction, only recently have some Member States begun to mobilize, expressing strong concerns about the impact of online addiction on children's health.

10.2.5. CEN/CENELEC

In September 2023, European Standardisation Organisation CEN/CENELEC issued a basic document with practical directions for programmers and designers of products and services to ensure that they respect children's rights when developing digital services. Workshop Agreement CEN-CENELEC CWA 18016 with the Institute of Electrical and Electronic Engineers (IEEE) regards the Age-appropriate digital services framework and was signed by various agencies such as 5Rights Foundation and Eurochild.

This is based on standard 2089 of IEEE which is the framework for Age-Appropriate Digital Services. It is a framework that takes into account the principles of 5rights Foundation, which has issued best practices for the implementation of DSA for children and is available at https://5rightsfoundation.com/resource/5rights-launches-tool-to-support-dsa-enforcement-for-children/ .

Moreover, the IEEE standard provides procedures for digital services used by children, making services age-appropriate and creating a digital environment that supports children's safety and privacy by design. Therefore, children's rights and wellbeing, as described in general comment 25 (2021) of UNCRC, are taken into account at the early stages of developing a product or service, thus mitigating risks and enhancing benefits of the digital world for children under the age of 18.

11. Other EU Member State initiatives

At the Member State level, the United Kingdom has been a pioneer in adopting relevant legislation. In September 2020, the Age-Appropriate Design Code (AADC) was adopted, followed in 2022 by the Children's Code Design Guidance and in 2023 by the UK Online Safety Act, certain provisions of which came into force on October 31, 2024. The UK government has taken a significant step toward online safety by instructing the country's digital regulator, Ofcom, to make safety by design a cornerstone for the implementation of the Online Safety Act. Peter Kyle, the Minister for Science, Innovation, and Technology, announced today that safety by design will be the first legal strategic priority for implementing the Act.

In his statement, Kyle instructed Ofcom to ensure that digital platforms design their services with a focus on the safety of children. This directive requires Ofcom to report to the government on how its activities align with this objective. The announcement emphasized that platforms must "consider all aspects of their services and business models, including algorithms and functionalities, when thinking about how to protect all users online." Additionally, platforms are expected to "embed safety outcomes in the design and development of new features and functionalities and explore ways to make existing features safer."

Furthermore, the government announced the launch of new research on online harms, with the first project examining the impact of smartphone and social media use on children. This initiative aims to provide insights that will guide future policies and regulatory measures to improve online safety for young users.

Similar approaches have been adopted in Ireland, the Netherlands, France, and Sweden, with guidelines for protecting children in the digital space.

In Ireland, a 2020 guide was issued on European children's rights regarding online privacy and safety, titled Know Your Rights - A Guide to Children's European Rights to Online Privacy and Safety, as well as The Fundamentals for a Child-Oriented Approach to Data Processing in 2021.

In the Netherlands, a Code for Children's Rights was issued in 2021.

In Sweden, the Guide on How to Make the Internet a Safer Place for Young People was announced in 2020.

The German Act for Youth Protection (Jugendschutzgesetz) was updated in 2021 to tackle digital challenges and protect minors from risks such as internet addiction, internet bullying and harmful content. Some basic (non-exhaustive) points are:

- ✓ Protection from online risks: Digital platforms, including social media, video platforms and online games must take measures to protect minors from online bullying, grooming and exposure to harmful content.
- ✓ Prevention of online addiction: the Act makes clear reference to addictive mechanisms such as reward systems and spam that may lead to excessive use or addiction. Platforms must use features that prevent nonstop use by minors.
- ✓ Age-appropriate content and guidelines: platforms must provide clear age assessments and warnings for content, ensuring that minors are not exposed to inappropriate content. Parental control tools are also enhanced.
- ✓ Increased transparency: providers must be transparent regarding risks involved in their platforms and should provide clear explanations about personal data and privacy setting for parents and minors.

The French Act for Parental Control (2022-300/2022, Loi n° 2022-300) was amended in 2022 to enhance online children's protection and requires manufacturers to install parental control systems to online devices sold in France, whereas a decree was issued (Décret n° 2023-588) for implementation thereof as of 13 July 2024.

This amendment requires that all devices (such as smartphones, tablets, PCs and gaming consoles) used by children be equipped with parental control software. This act's goal is to assist parents in managing children's screen time, monitor children's online activities and prevent excessive use of digital devices. The main points include:

- ✓ Compulsory parental control software: manufacturers must install in advance or provide easy access to parental control tools in all devices. Such tools must allow parents to monitor and mitigate screen time, block inappropriate content and monitor device use.

- ✓ Easy use: the act underlines that parental control features must be easy for parents to set and manage without technical knowledge requirements.
- ✓ Privacy protection: along with monitoring, software must respect privacy of children and parents, ensuring that personal data are managed safely according to personal data regulations.
- ✓ Awareness campaigns: the French administration has also started information campaigns to educate parents on the importance of parental control use and responsible management of children's digital habits.
- ✓ Prevention of digital excessiveness: this act aims mainly at preventing excessive screen use that could have negative impacts on children's physical and mental health. The act encourages a balanced and healthy use of digital devices by children.

Also, **France's Data Protection Authority** (CNIL) has issued Recommendations for Online Protection of Children in 2021 and Recommendations for the design of mobile phone applications in 2024.

The French Act for digital age of consent (2023-566/2023), approved in June 2023, defines "digital adulthood" for social media use. The digital adulthood is set at 15 years of age, which means that minors under 15 need an explicit consent of their parents to register and use social media platforms. Setting the digital adulthood age creates a legal framework as to when minors may use social media platform independently, protects younger users and standardises requirements for online services in France.

Age limit at 15 years:

The act provides that minors under 15 years of age cannot use social media without parental consent.

From the age of 15 and above, minors may register to and use social media without parental consent. Potential parental control through applications is left at discretion.

Objective of the Act:

The objective is to protect minors from the risks of social media, such as exposure to inappropriate content, addiction, online bullying and privacy violations.

This act enhances the need for greater parental supervision of the use of social media by younger users.

Compliance with EU Regulations:

The digital adulthood age of 15 is higher than the minimum of 13 provided in GDPR, yet within GDPR allowed range (13 to 16 years of age).

France utilised the potential provided by GDPR to set a stricter age limit for digital consent.

Legal Consequences:

Social media platforms are obliged to implement age verification mechanisms to comply with legal requirements and ensure that users under 15 years of age have parental consent.

Non-compliance may incur fines and penalties by competent French regulatory authorities like ARCOM.

12. European and International Practices

12.1. European (Member States and EU)

Parental control and screen time monitoring applications: throughout the EU tools like Qustodio and Google Family Link are broadly used to allow parents to manage their children's online activities. Such applications provide specific methods for monitoring application use, set screen time limits and receive reporting on digital behaviour. This helps children manage their online time and avoid addiction.

Safer Internet Centres (SIC): they are the main component of the initiative Better Internet for Kids (BIK) that is coordinated by the European Commission. SICs operate in EU Member States** and some neighbouring countries and provide various services that promote digital wellbeing, online safety and a positive digital environment for children, parents and teachers.

Hotlines for parents and children:

Many SICs provide Phone Hotlines for children, parents and teacher to ask for advice and support regarding concerns for online safety, including internet addiction. Such hotlines offer practical advice on how to mitigate screen time, online games and social media addiction management. For instance, the Belgian Safer Internet Centre offers a special hotline for families to adopt healthier digital habits.

Digital education curricula at school:

Many EU countries integrate digital literacy education into school curricula. These programs teach students to recognize signs of addiction, responsibly manage online time, and constructively use digital platforms. In Finland and the United Kingdom, for example, students participate in workshops analysing their own screen time and developing healthier digital habits.

Since the Age-Appropriate Design Code was put in force in the UK in September 2021 a number of changes was seen in technology product design which improved children's digital experience. Instagram prohibited adults from sending messages to children. It also deactivated location monitoring and introduced reminders for children to take breaks. Google made SafeSearch a standard operation for children and deactivated autoplay videos on YouTube. TikTok recently set private accounts as default for individuals under the age of 16. These changes are implemented regionally or internationally and now the next step is to set a worldwide standard for regulating technology for children focused on privacy protection, safety and autonomy in the digital sphere.

12.2. International

A remarkable act is the California Consumer Privacy Act (CCPA) with special provisions for children's data protection, as a business can sell private information of a child under the age of 16 only following consent. For children under 13 years of age this approval must be made by a parent or legal guardian, whereas children between the ages of 13 and 16 must provide their own consent.

Subsequently, California became the first US State in 2022 to introduce the entire UK Age-Appropriate Design Code and passed an Act regulating online activities of all children under the age of 18. It is the California Age-Appropriate Design Code Act ("Design Act"), which imposes additional compliance requirements for companies offering products and services to children. Maryland and Vermont followed this example.

Indonesia passed two acts early 2024 for online children's protection. Those acts provide for the activation of an Age-Appropriate Design Code following UK standards. The Code is at the final stage of processing (by the Ministry Communication and Informatics) and is due for signing early 2025 by the President of the Indonesian Republic.

Australia has also introduced such an act in 2021 (Australian Online Safety Act), with special provisions for children's safety and obligations for online service providers to develop new industrial codes and standards.

The Australian Parliament approved a milestone draft law in November 2024, which aims at banning children under the age of 16 from social network platforms, leaving the final decision to the Senate to ratify this pioneer legislation.

The law, which received bipartisan support, places significant responsibility on platforms such as TikTok, Facebook, Snapchat, Reddit, X, and Instagram, holding them accountable for fines of up to 50 million Australian dollars (approximately 33 million USD) in cases of systemic failure to prevent the creation of accounts by children under the age of 16. The legislation was approved with 102 votes in favor and 13 against. If the Senate passes the bill and it becomes law, social media platforms will have a one-year period to implement the necessary measures to enforce age restrictions before penalties begin to be imposed.

Opposition MP Dan Tehan informed Parliament that the government had agreed to Senate amendments aimed at strengthening privacy protections. Specifically, the amendments will prohibit platforms from requiring users to submit government-issued identification documents, such as passports or driver's licenses, or mandating identification through a government digital recognition system.

12.2.1. China

On October 24, 2023, China's State Council fully released the "Regulations on the Protection of Minors Online." This appears to be the world's first comprehensive national legislation regulating the protection of minors online. Based on the principles of maximizing the benefit for minors and promoting social co-governance, the regulations comprehensively establish fundamental systems in the field of online child protection, such as cultivating online literacy for minors, standardizing online content, protecting the personal information of minors, and preventing online addiction. This requires thorough study by government departments, parents, schools, and other stakeholders.The regulations also emphasize the primary responsibility of platform businesses, setting the direction for building a compliance system for the protection of minors by online enterprises in China. These regulations not only promote the positive role of platform businesses in safeguarding minors online in China but also contribute to disseminating "Chinese wisdom" in exploring new mechanisms for protecting minors online in the digital era for all of humanity.

12.2.2. OECD work for children in the digital environment

The OECD's work on children in the digital environment began with the Seoul Ministerial Declaration of 2008, which called for a collective effort "among governments, the private sector, civil society, and the Internet's technical community to build understanding of the impacts of the Internet on minors to strengthen their protection and support while using the Internet."In 2011, the OECD published a detailed report analyzing the risks faced by children in the digital environment at that time, and in 2012, it adopted a recommendation for the protection of children online.

Subsequently, in 2020, an OECD study found fragmented legal and policy responses to children's needs in the digital environment, as well as an evolving and complex risk landscape. It highlighted that parents need support to help their children navigate the digital world and that children's opinions should be sought and recognized as key stakeholders and rights holders in the development of policies. It also noted that reliance on co-regulation or self-regulation by digital service providers was inadequate to meet children's needs, emphasizing the critical role of these providers in ensuring a safe and beneficial digital environment for children.

On May 31, 2021, building on these findings as well as technological, policy, and legal advancements since 2012, the OECD Council issued the Recommendation on Children in the Digital Environment (a revision of the 2012 version). This recommendation outlines key principles and provides specific guidance to governments and other stakeholders to achieve a safe and beneficial digital environment for children. The OECD Guidelines for Digital Service Providers, adopted alongside the recommendation (as an addition), aim to support digital service providers in taking measures that respect and protect children's rights, safety, and interests. The OECD recommendation is accompanied by a supplementary document that offers guidance and a framework for governments and stakeholders to support implementation efforts.

Many very large platforms of entertainment and information face complex situations in the protection of minors. Online platforms with a large number of minor users or a substantial influence on the group of minors should not only conform to the requirements of all systems provided in regulations, but also meet special requirements in six fields:

- ✓ Adaptation of services to the physical and psychological characteristics of minors at various stages of design, research, development and operation, and regular assessments of online impact on minors.
- ✓ Provision of a special mode for minors ("Minors' Mode") and a special zone of services for minors, with an appropriate legal basis for both.
- ✓ Establishment of a compliance system for online protection of minors, with an independent agency comprising mainly outsourced members to supervise protection status.
- ✓ Drafting of new regulations for protection of minors, notifying in a visible manner minor users about their rights for protection and about potential harm.
- ✓ Immediate suspension of products or services that violate legal rights and interests of minors.

✓ Issuance of an annual special report of social responsibility for the protection of minors online.

The above requirements will assist businesses to play the main and leading role in the protection of minors online and will improve the overall level of protection in the country.

Clear requirements for smart terminal devices

Digital products and services develop very fast, with big differences in the operation for protection of minors they offer. Enhancing protection features for smart terminal devices helps to improve protection of minors online in the entire digital field. According to 51st Statistical Report on China's Internet Development by the China Internet Network Information Centre internet users via mobile phones rose up to 1,065 billion in 2022.

Regulations provide that:

✓ The state encourages and supports the development of products adapted to physical and psychological characteristics of minors.

✓ Related products must be equipped with functions like identification of inappropriate content, privacy protection, addiction prevention and facilitation for guardians.

✓ All products must have software for protection of minors, either a standard feature or with clear download directions.

Such regulations promote better contribution of businesses manufacturing smart devices to online minors' protection.

New Requirements for Online Information Content

On the basis of the emphasis of the state to enhance dissemination of positive energy and prohibit the dissemination of harmful material, regulations set four specific requirements for online businesses:

✓ Establish basic standards for the content that may affect minors' physical and mental health. Regulations include four content types to avoid: content promoting unsafe behaviours, violations of social ethics, extreme emotions or development of bad habits.

✓ No harmful content at visible places, such as main pages, popup windows or top searches.

✓ Prohibition of commercial targeting of minors through automated decision-making methods.

✓ Immediate tackling of harmful content, including erasing, blocking or reporting to competent authorities. Users that produce or disseminate such content must be subject to warning, operation restrictions or even account shutting.

Clear Requirements for Prevention of and Addressing Online Bullying

Online bullying affects greatly the physical and mental health of minors and has been an issue of international attention. Regulations provide specific requirements from online businesses:

✓ Set up a mechanism to prevent and identify online bullying using AI, big data and a combination of technology and human supervision.

✓ Ensure easy access to operations for storing evidence and exercise rights by minors and parents.

✓ Provide minors with self-protection tools, such as blocking unknown people, visibility of posts and avoidance of messages by third parties.

✓ Take measures against users that disseminate online bullying material.

Enhancing the Protection of Minors' Personal Data

Regulations underline the importance of protecting minors' personal data, based on Personal Data Laws. They determine three specific requirements:

✓ Facilitate access, correction or erasure of data by minors or their parents.

✓ Annual compliance checks for the processing of personal data of minors, and submission of results to competent authorities.

✓ Address sensitive incidents, such as private messages of minors, through special measures (notifications, filing or reporting to the authorities).

New Requirements for Prevention and Addressing of Internet Addiction

Internet addiction greatly affects the health and development of minors. Regulations include six requirements for online businesses:

✓ Set addiction prevention and addressing systems at the design, development and operation of products.

✓ Immediate amendment of products with addiction risks.

✓ Annual public reporting for prevention and addressing addiction.

✓ Implementation of "Minors' Mode" in games, livestreaming and social networks.

✓ Restrictions to internet services use by minors.

✓ Use of electronic identification for age verification and implementation of age-appropriate systems.

Emphasis on Setting an Effective Complaints and Reporting Mechanism for Minors' Protection

Regulations require that online businesses:

✓ Set up simple and effective channels for complaints and reports, with clear access directions.

✓ Quickly collect and manage complaints and reports.

✓ Provide professional training to the staff that manages complaints, so that they understand related legislation and effectively manage incidents.

Serious Legal Liabilities for Violations of the Obligations for the Protection of Minors Online

The lack of strict penalties for violations of laws in the field of minors' protection raises concerns. Regulations determine various degrees of liabilities:

✓ Minor violations: Compulsory correction and reporting to authorities.

✓ Serious violations: Big penalties, such as high fines, resume of activities, website shutdown or revocation of operation permits.

✓ Liabilities of Natural Entities: Fines and employment restrictions.

The goal of such strict penalties is not to punish but to encourage businesses to put priority in the protection of minors and implement legal requirements on time.

Strategic Approach to Enhance the Protection of Minors by Businesses

Businesses are proposed to act timely in three sectors:

✓ Establish an internal mechanism of minors' protection: high-rank executives of businesses should take leading roles and incorporate the protection of minors in strategic planning and main decisions.

✓ Cooperate with independent agencies: businesses should appoint third parties to make special assessments for the protection for minors, so that problems are timely identified.

✓ Extensive compliance: legal requirements must become internal rules and procedures, incorporating law in all aspects of business development.

12.3. Case Studies of smartphones prohibition

12.3.1. United Kingdom

In 2023 the possession of smartphones in the United Kingdom was almost universal (98%) up to the age of 12 years, and this was boosted by the transition from primary school to secondary school. There had been requests for data-based guidance to schools, in order to inform the development of policies regarding the use of smartphones. Recent non-statutory guidance proposed by the Department for Education (DfE) reads:

"Every school has a duty to create an environment that is calm, safe and free from distraction so all pupils … schools should develop a mobile phone policy that prohibits the use of mobile phones and other smart technology with similar functionality to mobile phones … throughout the school day, including during lessons, the time between lessons, breaktimes and lunchtime"

Nevertheless, there is a substantial differentiation among schools regarding the implementation of policies for smartphones. A recent review of smartphone policies in the UK classified school responses into four categories, and found that, among secondary schools:

✓ 11% implemented what they term an 'Effective ban' (where phones are not allowed in or are stored in lockers or equivalent, e.g., Yondr pouches, at the start of the day);

✓ 52% "Ban, but phone present" (e.g., in school bags);

✓ 36% "Partial ban" (phones banned in class, but allowed at some times, such as break or lunch);

✓ Finally, no schools reported having 'No ban'.

When mapped against current school ratings, as awarded by Ofsted, the schools' regulator, an informal selection of schools rated as "Outstanding" were more likely to impose general restrictions on smartphone use within school premises. Schools rated as "Requires Improvement" adopted a variety of approaches, often simply telling students that smartphones must not be used, seen, or heard during the school day. Schools rated as "Good" typically required students to hand in their phones upon arrival or ensured that they were not accessible during the school day (e.g., through the use of a personal Yondr pouch or equivalent).

Given the growing interest in Yondr pouches (or a similar variant), it is worth noting that these are considered the property of the school, but students are responsible for bringing the pouch with them to school each day and keeping it in proper working condition.

12.3.2. Singapore

As with children in the UK, children in Singapore alike will probably have their first smartphone between 9 and 12 years of age. Unlike countries that wish to ban or restrict smartphones, the Singapore Ministry of Education will require all students to have their own digital device by 2028. Students will pay for the device through their Edusave accounts (where the state contributes an estimated USD 75m per annum). Students who need financial aid will be provided with state subsidies to cover the full cost of the devices. Each device, either a smartphone, tablet or laptop, will be equipped with management software, not only to prevent misuse but also to enhance digital literacy courses in class.

This initiative is based on Singapore's wish to consider digital education "in a deeper and more holistic way". Digital literacy will be incorporated in the curriculum, instead of being a separate discipline. Students are expected to use their devices and acquire skills in various disciplines, as described in their curriculum, which will allow them to:

✓ Collect and critically assess information from digital resources in a safe, responsible and ethical manner,

✓ Interpret, analyse and resolve problems systematically,

✓ Use software and devices effectively and productively,

✓ Facilitate the use of knowledge and skills in new contexts and follow technological developments,

✓ Produce content and cooperate with others in digital environments.

The Singapore Student Learning Space platform is an online educational tool that enhances the learning experience through the targeted use of technology. Students can learn at their own pace, while any difficulties or challenges can be more easily identified by their teachers and addressed early. Despite the optimism and positive indications that such an approach can improve classroom learning outcomes, recent research has highlighted issues such as unfair data practices, including tracking and ranking children, a lack of transparency, and complexities surrounding data processing and management.

As children grow older and gain more independence, parents are eager to use digital devices and services to stay connected. However, such practices must be implemented with care, as the increasing integration of smartphone communication into parental monitoring can introduce problematic tensions in the parent-child relationship.

During the **Covid-19 pandemic**, online learning clearly exposed the challenge of the digital divide, as many students initially lacked devices to participate in remote education. Schools loaned over 20,000 smart devices to students, while community organizations also donated technology. After addressing access gaps, schools in Singapore are now working to bridge learning outcome disparities, viewing the future of education as an opportunity to leverage the power of technology and smartphones as educational tools.

It is noteworthy, however, that while the government's official policy encourages the educational benefits of digital devices, some schools implement "bans" or restrictions on smartphones in various ways. At tutoring centres, smartphone policies are likely to be more liberal compared to regular schools, but they shape students' expectations about what they can or cannot do with smartphones in educational settings.

12.3.3. Colombia

In the context of its commitment to the wellbeing and development of students, the Union of International Schools (Uncoli) and 27 private international schools that are its members (with approx. 17,000 students), have agreed to apply a restriction to smartphone use during schooling hours. Each Uncoli school can develop and implement its own detailed policy on restriction, adapted to the local framework and student needs. The reasons they present on their website refer to research findings that support that devices:

- ✓ Are linked to reduced academic performance.
- ✓ Have a negative impact on mental health.
- ✓ Reduce the quality of social interactions.
- ✓ Increase bullying and online bullying.
- ✓ Contribute to developing addictive behaviours.
- ✓ Reduce interest in physical activity.

The Ministry of Education replied to the joint declaration of Uncoli by supporting that the use of screens and smartphones in class must contribute to the development of academic activities. Before the implementation of a similar measure for all schools in the country, the Ministry insists that there should be dialogue and agreement within each academic board, including principals, teachers, students, even parents, to determine whether smartphone use should be mitigated. The Constitution is the most important regulation in the legal system of Colombia and each provision is in line with its content. According to Article 44 of the Colombian Constitution: family, society and State are obliged to assist and protect children and to guarantee their balanced development and full exercise of their rights.

Therefore, current regulations indicate that smartphones should not be available for minors under the age of 14; nevertheless, there are no explicit regulations that prohibit parents or schools from providing smartphones. The regulatory approach of Colombia is formulated a) by Act 2170, which stipulates that every person has the right to communicate with others using speech, writing or symbols, or through the application of tools provided by ICTs, and b) by a provision that allows schools, by exception, to limit the use of smartphones, if this does not violate the right of students for communication. This includes:

- ✓ Freedom of expression and propagation of thoughts and opinions.
- ✓ Free development of personality.
- ✓ Ability to inform and receive true and impartial information, education and access to knowledge, science, technology and other goods and values of civilization.

This is done to protect students in dangerous situations related to the use of technological and communication devices, in accordance with building a culture of protection pursuant to Act 1098 (Code of Childhood and Adolescence).

Moreover, for individuals between the ages of 14 and 18 years, article 45 stipulates that teenagers have a right to balanced development and protection. Further, article 7 of Act1581 (2012) names several agencies to be responsible for ensuring online safety of children and adolescents, particularly as regards data and privacy. The Court of Law stated that it should be understood that:

- ✓ Not only the State and schools should develop actions to prevent inappropriate use of personal data of minors under the age of 18, but also:
- ✓ Parents and other individuals that are responsible for their care, and teachers being responsible for guaranteeing this.
- ✓ The legislator, who must ensure that (in the context of his legislative work, especially as regards private data of children under 18) legislation includes appropriate protection measures for children's balanced development and effectiveness of fundamental rights, as described in the Constitution and international standards.
- ✓ The judiciary systems, and particularly civil servants, must protect the rights arising from the use of personal data of children under the age of 18, observing international standards or specialised document on this matter.
- ✓ The media agencies.
- ✓ The companies that provide internet access services, develop applications or digital social networks, are warned of their commitment to protect fundamental rights of children and adolescents.