OPEN LETTER[1] REGARDING THE UPCOMING LEGISLATIVE PROPOSAL TO BAN ACCESS TO SOCIAL MEDIA FOR CHILDREN UNDER THE AGE OF 15

Athens, 19.05.2026

To:

-Prime Minister of the Hellenic Republic, Mr Mitsotakis,

-Minister of Health, Mr Georgiadis,

-Minister of Digital Governance and Artificial Intelligence, Mr Papastergiou,

-Minister of Justice, Mr Floridis,

-Minister of State, Mr Skertsos

CC:

-Minister of Education, Religious Affairs and Sports, Ms. Zacharaki

-Minister of Social Cohesion and Family, Mr. Michailidou

A. Introduction

We, 25[2] Greek and international organisations, hereby sign and address this letter to you in order to express our substantiated concerns regarding the proposed imposition of a ban on access to social media for children under the age of 15 within the Greek territory, as announced on 8 April 2026 and published on 12 May 2026 in the context of the TRIS procedure on the relevant platform of the European Commission.

We understand that this legislative initiative has understandable concerns as a starting point. However, legislative initiatives that focus on horizontal bans based solely on age raise serious questions of proportionality, potential adverse impacts on the Rights of the Child and on the rights of the population as a whole, and ultimately, of scientific substantiation. Significant concerns regarding such horizontal bans have been consistently expressed, inter alia, by:

- the Council of Europe Commissioner for Human Rights,
- more than 400 academics and experts in the field of information technology,
- reputable scientific bodies, such as the National Academies of Sciences, Engineering and Medicine (NASEM), the international network EU Kids

[1] The main letter is accompanied by an annex, which provides a more detailed explanation of the ten concerns referenced in Section C.
[2] The Electronic Frontier Foundation and the Defend Digital Me co-signed the joint letter one day after its submission, as an expression of support for the initiative, specifically on 20 May 2026.

Online of the LSE, and the scientific journal of digital health and informatics *The Lancet Digital Health*,

- Eurochild, the largest network of organisations and individuals in Europe working for children,
- an alliance of 42 child protection and online safety organisations, and
- an alliance of 28 youth organisations from across Europe, including the Hellenic Youth Council (ESYN), as well as the European Digital Rights (EDRi).

The effectiveness of legal frameworks for the protection of children under the age of 15 in the digital world should not be assessed on the basis of the number of those excluded, but rather on the extent to which their access to safe environments that respond to their real needs is ensured. Prohibiting children from accessing social media does not eliminate the risks they face online, rather it merely delays their exposure to unsafe and unhealthy environments while the underlying harm remains unaddressed.

B. Brief outline of our concerns regarding your legislative initiative

We set out ten (10) concerns arising from the proposed regulation, which are further elaborated in the Annex to this letter:

(1) The scope of application of the measure concerns all users, regardless of age

The proposed ban does not affect only children under the age of 15. According to the Press Release, and in particular the Ministry of Health's Q&A document, "upon implementation of the law, platforms will be required to proceed with a scenario of age 're-verification' of all accounts in Greece, so that accounts with a declared age different from the actual one and below the established thresholds will be excluded from the use of Social Media." During the press conference, Mr Papastergiou stated (from 39:00 onwards) that this re-verification will be made possible by platforms through tools such as algorithms. Of course, technology companies have been collecting our data for years for advertising purposes. However, this development goes a step further. The proposed legislation transforms what has so far been a practice of commercial data exploitation (specifically, the practice of collecting data to build age-group profiles) into an absolute obligation for social media providers, upon which the ability of users to retain access to the services they offer will now depend. In this way, user monitoring and the obligation to create profiles cease to be a by-product of the commercial practices of specific internet giants and tend to become a structural feature of maintaining access to the digital space. Furthermore, as more than 400 academics and experts in the field of electronic services note in their joint letter, the use of digital age-verification wallets for access to digital platforms, even if currently accompanied by privacy-enhancing measures, may lead to significant challenges for online anonymity in the future. In an interview with inside.story, one of the world's leading cryptographers, Professor Bart Preneel, characteristically stated: "gradually all services on the internet at the European level will acquire an entry barrier, therefore the consequences will be enormous for everyone. […] If you want to get rid of anonymity on the internet, you must first put a 'door' on every service, because the internet currently has no 'doors'. So you start with one 'door' and with a state-controlled application, and in the future it is not difficult for this application to be updated in a way that the identity [of the user] can be revealed." Therefore, as access to services becomes dependent on prior identity verification through specific "entry gates," such as digital wallets in this case, this development may lead not only to a restriction of anonymity but also to a reconfiguration of the very architecture of the internet, with potentially far-reaching negative consequences for fundamental rights in the digital space.

(2) Non-transparent handling of the relevant recommendation of the competent committee of the Central Health Council (KESY)

Following a request from the Ministry of Health, the competent Mental Health Committee (ΕΨΥ) of the Central Health Council (KESY) appointed a four-member group of experts, chaired by the distinguished Dr Striggaris, to formulate guidance regarding "the use of smartphones and social media by minors up to the age of 13." The expert group submitted a substantiated recommendation on 20 March 2026, which was unanimously approved by the ΕΨΥ and subsequently referred to the Plenary of KESY. However, the announcement of the measure on 8 April intervened abruptly, without any commentary on the arguments presented, or even a simple acknowledgment of the existence of the aforementioned recommendation. While such opinions are not binding on the government, in this case it appears that they were not taken into consideration at all. Dr Striggaris has summarized these developments in a relevant public post. The following point (3) makes specific reference to the content of this recommendation.

(3) Lack of participatory and evidence-based lawmaking

Unfortunately, the measure does not comply with the principle of participatory lawmaking, as it has not been accompanied by the involvement of citizens and stakeholders during the legislative drafting process. According to publicly available information, no tools for gathering views, such as public consultations or questionnaires, have been utilized, nor have thematic meetings or

consultations been organized with the participation of competent authorities, experts, academics, civil society, and children themselves, as is in fact provided for under Article 12 of the United Nations Convention on the Rights of the Child (Law 2101/1992, hereinafter "the Convention"), which is binding on the Greek State. Moreover, the principle of evidence-based lawmaking is not being respected. Specifically, the development and implementation of such a measure cannot be considered justified unless it is clearly demonstrated that the expected benefits substantially outweigh any potential harmful consequences. Undoubtedly, certain clinical and psychosocial findings concerning social media should be acknowledged, particularly those relating to emotional irritability and aggression, disengagement from the educational process, as well as body image and the formation of children's identity. However, as discussed above (point 2), the only relevant expert recommendation from KESY appears not to have been taken into account at all. In particular, in a relevant interview with inside.story, Dr Striggaris notes that the recommendation provided a thorough analysis showing that the current consensus in the international literature is that, for the general population of children and adolescents, a causal link between social media use and mental health has not been sufficiently established. He further explains that, according to the precautionary principle, legislators may adopt measures even where a causal link cannot be fully proven. However, at this point, the issue of proportionality arises, which is of particular importance in light of contemporary conditions, as we live in a digital era in which children are expected to become familiar with the digital world, which now constitutes an integral part of the public sphere. Consequently, the recommendation concluded that the imposition of blanket bans may lead to unforeseen and potentially adverse consequences for children. For this reason, the experts emphasized in their recommendation that developments in countries such as Australia should be carefully monitored, and that policymakers should await the availability of reliable data before making final decisions. Finally, any proposed measure should be accompanied by provisions for the systematic scientific assessment of its impact. Although domestic research remains limited, as already noted above, international experience from countries such as Australia and the United Kingdom may provide useful comparative data for the evaluation of similar policies.

(4) Socio-economic exclusion and incompatibility with the principle of non-discrimination

Existing age-verification methods generally presuppose the use of a modern "smart" mobile device, as well as the possession of adequate digital skills, particularly on the part of children's parents. A reasonable question therefore arises as to whether parents who do not possess such devices or lack the necessary digital skills will be able to comply with the proposed measure. Similarly, individuals who do not possess identity documents are unable to meet the requirements of most age-verification tools, with the result that they are excluded from access to basic means of communication with their relatives within the Greek territory.

(5) Disproportionate interference with the Rights of the Child

Age-based restrictions may constitute a disproportionate interference with the fundamental rights of children. In particular, a restriction on the ability of children under the age of 15 to exercise their rights to information, expression, and association online, such as the one proposed, could be in conflict with Articles 13 and 15 of the Convention, as well as with Articles 11 and 12 of the Charter of Fundamental Rights of the European Union. Relevant arguments are also set out by the United Nations Committee on the Rights of the Child in its General Comment No. 25, entitled "Children's rights in relation to the digital environment" (paras. 50–66), while a comprehensive account of the various rights of child users that are directly affected by such legislative initiatives is also provided in a recent study by the European Union Agency for Fundamental Rights.

(6) Risk of displacement of children to non-compliant platforms and easy circumvention of measures through technical means

As argued by more than 400 academics and experts in the field of information technology, age-verification mechanisms can be easily circumvented, as demonstrated by existing applications that are bypassed through the use of virtual private networks (VPNs). In this way, child users could be exposed to additional risks. As is well known, VPN providers that offer their services free of charge typically collect and process users' personal data in order to sell it to data brokers, which in turn leads to profiling and significant challenges for privacy. Furthermore, as also noted by the Network for Children's Rights in a relevant statement, children who circumvent such restrictions are particularly unlikely to report incidents they may encounter on those platforms, for fear of revealing their "irregular" presence.

(7) Unclear announcements regarding the proposed regulation, which hinder public debate and may create misleading impressions in relation to the proposed text of the Draft Law

Unfortunately, certain unclear, and even contradictory, positions are observed regarding the proposed measure, which require further clarification. First, the Press Release (PR) of the Ministry of Health states, already in its opening paragraph, that "the draft bill under preparation introduces a clear and coherent framework for the protection of minors in the digital environment, fully aligned with European law and the guidelines of the European Union." However, in the very same publication, this time within the Q&A section, the Ministry of Health appears to contradict this statement, as it notes that "time is required to assess whether the proposed measure can be implemented without creating legal or operational conflicts with the European framework," an approach that reflects reality, given that the applicable legal framework raises complex issues of compatibility (see point 8) and for this reason the TRIS procedure is also being followed. Second, under the proposed legislative initiative, "access to online social media services is prohibited." However, the EU legal framework defines, in the Digital Markets Act (DMA), the concept of an "online social networking service" in a horizontal manner. Thus, as evident from the Draft Law published on the TRIS platform, and in particular from Articles 3 and 4 thereof, the proposed regulation will indiscriminately cover also decentralized online platforms of the so-called Fediverse, such as Mastodon or PixelFed. These platforms operate under a different business and technological model compared to dominant social media services; they are not based on a central

corporate structure and, as a rule, do not employ technical and design practices that promote addictive use. Finally, since under the DMA the service category of an "online social networking service" is distinct from that of a "video-sharing platform service," platforms such as YouTube do not legally qualify as social media services and, therefore, the Greek Government has chosen not to include them in the proposed regulation. Since the measure, pursuant to Article 1 of the Draft Law, aims to protect mental health of users from addictive designs, the rationale for excluding certain platforms should be clarified and substantiated on the basis of quantitative and qualitative data, which are absent from the announcements of the Greek State.

(8) Obligation to comply with the applicable EU legal framework

It is important to highlight that, unfortunately, at the time the measure was announced on 8 April, there was no clarity regarding either the content or the mandatory nature of the proposed measure. In particular, based on the Press Release and the Q&A document published by the Ministry of Health, it was understood that, from January 2027, platforms will be required to proceed with a scenario of age re-verification of all accounts in Greece, so that accounts with a declared age different from the actual one and below the established thresholds are excluded from the use of social media and are required to undergo verification through a tool such as the "Kids Wallet." However, in statements made during the same press conference, Mr Papastergiou indicated that, ultimately, there will be no such obligation imposed on platforms to use the "Kids Wallet" (from 24:40 onwards and 49:17 onwards). Ultimately, the Draft Law published on the TRIS Platform on 12 May provides, in Article 4(3), that: "Providers of online platforms offering online social networking services shall implement appropriate, proportionate and reliable age-verification methods, including the equivalent European Union age-verification solution, which is integrated into the 'Gov.gr Wallet' application under Article 80 of Law 4954/2022 (Government Gazette A' 136) and into the 'Kids Wallet' application under Article 80A of Law 4954/2022, with the aim of restricting access to users who have not reached the age limit provided for in paragraph 1," namely 15 years of age. Furthermore, pursuant to paragraph 4 of the same Article: "Providers of online platforms offering online social networking services may complement age-verification techniques with age-estimation methods, where deemed necessary to ensure a high level of privacy, security and protection of minors." Therefore, it must first be assessed by the European Commission whether the proposed measure creates new obligations for platforms, or whether Article 4(3) merely restates the existing obligations arising from Article 28(1) and Article 35(1)(i) of the DSA. In any event, Article 4(4) does not create any actual obligation, since it contains the term "may" and therefore constitutes a proposed self-regulatory measure without any binding force. It should be emphasized that, depending on the nature of the obligation, issues of compatibility could arise not only with the Digital Services Act (DSA), but also with the principles of the country of origin and mutual recognition under Article 3 of the Directive 2000/31/EC, which remains in force alongside the provisions of the DSA. Similar concerns have been raised by legislators in other Member States, such as France and Germany. Finally, it must be stressed that, within the EU legal order and in Greece, a legal framework already exists but is not adequately enforced. Since 2019 in Greece, through the implementation of Article 8 GDPR in Article 21 of Law 4624/2019, children under the age of 15 benefit from enhanced protection with regard to the processing of their personal data in the context of information society services, where such processing is based on consent. However, in practice, large digital platform companies, since the entry into force of the GDPR (May 2018), have systematically sought to shift the legal basis for processing, opting for legitimate interest or the performance of a contract in order to circumvent the relevant protective obligations, thereby violating EU law. Similarly, the specific safeguards provided for in Article 28 of the Digital Services Act (DSA), concerning the protection of all minors (without differentiation by age group), remain limited and ineffective. In its effort to strengthen the protection of children online, the Greek State could take a leading role in opposing the Digital Omnibus and Digital Omnibus on AI packages, which contain provisions that significantly weaken the framework for the protection of users in the digital environment.

(9) Cybersecurity challenges

Recent developments highlight that digital identity and age-verification applications are accompanied by significant cybersecurity challenges and technical vulnerabilities. Indicatively, just a few hours after the European Commission announced its new age-verification application, computer experts, speaking to POLITICO, raised a number of concerns regarding its design and level of cybersecurity, pointing to serious weaknesses and risks related to sensitive data breaches as well as identity theft. At the same time, a critical vulnerability was recently identified in the Greek digital wallet application Gov.gr Wallet, with Andronikos Koutroubelis, a graduate of the Department of Informatics of the Athens University of Economics and Business and co-founder of FactReview, notifying the National Cybersecurity Authority immediately upon its discovery, as reported in a relevant investigation by inside.story. The vulnerability existed from September 2025 until 22 April 2026, despite the competent authorities having been informed of the flaw as early as 30 March. Therefore, prior to promoting the widespread, and in particular mandatory, use of such tools, a thorough and independent assessment of their security and reliability is necessary, in order to ensure that no new, systemic risks to citizens' rights are created.

(10) Need for a substantive emphasis on alternative solutions

Strengthening education and digital literacy may constitute an appropriate and proportionate alternative to horizontal restrictive measures. Systematic information and awareness-raising among children regarding both the risks and the benefits of the internet, combined with the cultivation of critical thinking skills and responsible use, contribute substantially to their independent empowerment and to reducing their exposure to harmful practices. In this context, the development and implementation of targeted educational programmes, both within the school environment and at the family level, constitute a mild yet effective means of prevention. However, the proposed measure appears to lack the adoption of a multi-layered approach, which would include the education of children, as well as the promotion by the State of structured awareness-raising campaigns capable of strengthening children's critical judgment and meaningfully supporting parental guidance. We consider it absolutely necessary to develop educational interventions within the school environment aimed at fostering digital literacy and critical thinking, a sense of responsibility and self-regulation, empathy and social skills, sexual education, and the mental resilience of young people. Equally critical is the provision of information, training and support to parents and parents' associations, so that they may develop the necessary skills to respond effectively to the challenges of the digital age.

C. Our Requests

By means of this letter, we request:

(1) the organization of an inclusive and open consultation in order to discuss the direction of the proposed law. Such a consultation could take place at the premises of the Ministry of Digital Governance and Artificial Intelligence. In addition, the possibility of online participation for stakeholders based outside Athens could further enhance inclusiveness.

(2) the publication of the recommendation of the KESY committee. The content of this recommendation would inform the public debate with the necessary scientific arguments and the substantiated views of experts.

(3) official information regarding the existence or non-existence of other relevant expert opinions from the competent Ministries, particularly concerning the compliance of the measure with the EU legal framework and the required technical cybersecurity measures.

(4) any legislative initiatives to require platforms to redesign their harmful and extractive business models and ensure that platforms are safe and healthy for all users, regardless of age.

We look forward to your response and remain at your disposal for any clarification. Yours sincerely,

- Asociația pentru Tehnologie și Internet (ApTI)
- Alternatif Bilisim
- Amnesty International – Greek Section
- Chaos Computer Club Karlsruhe – Entropia e.V.
- Danes je nov dan, Inštitut za druga vprašanja
- Defend Digital Me
- Digital Democracy Foundation
- Electronic Frontier Foundation
- EPAPSY (Association for Regional Development and Mental Health)
- Epicenter.works – for digital rights
- European Digital Rights (EDRi)
- FactReview
- Hellenic Informatics Union (EPE)
- Hellenic League for Human Rights
- Homo Digitalis
- Initiative für Netzfreiheit
- In_contACT org
- IT-Pol Denmark
- Metamorphosis Foundation
- Network for Children's Rights
- Open Technologies Alliance (GFOSS)
- Research Institute for Regulatory Policies
- SHARE Foundation
- Union of Consumers “Quality of Life” (EKPIZO)
- Visible Machines - AI Research and Social Awareness Cent

Annex: Detailed Presentation of the Ten Concerns Set Out in Section C of Our Letter

(1) The scope of application of the measure concerns all users, regardless of age

The proposed ban does not affect only children under the age of 15. According to the Press Release, and in particular the Ministry of Health's Q&A document, "upon implementation of the law, platforms will be required to proceed with a scenario of age 're-verification' of all accounts in Greece, so that accounts with a declared age different from the actual one and below the established thresholds will be excluded from the use of Social Media."

During the press conference, in response to a question by journalist Sofia Christou from the newspaper Kathimerini regarding the process and the practical manner in which platforms will determine that an account does not reflect a user's real age, Mr Papastergiou stated (from 39:00 onwards) that "there are ways and processes, algorithms, to verify this," thereby indicating the use of algorithmic age profiling as a tool.

Of course, technology companies have been collecting our data for years for advertising purposes. Algorithms and continuous content-flow design features seek to capture and sustain users' attention, treating them as "products," as their data and online behaviors are exploited for commercial purposes. However, this development goes a step further. The proposed legislation transforms what has so far been a practice of commercial data exploitation (specifically, the collection of data to construct age-group profiles) into an obligation for social media providers, upon which the ability of users to retain access to the services they offer will now depend. In this way, user monitoring and the obligation to create profiles cease to be a by-product of the commercial practices of specific internet giants and tend to become a structural feature of maintaining access to the digital space. Moreover, this practice in itself increases privacy risks for all users, as data may be subject to misuse either by the provider itself or by third parties who may gain access to them, for example as a result of a data breach.

Furthermore, as more than 400 academics and experts in the field of digital services note in their joint letter, the use of digital age-verification wallets for access to digital platforms, even if currently accompanied by privacy-enhancing measures, may lead to significant challenges for online anonymity in the future. In an interview with journalist Eliza Triantafyllou for inside.story, one of the world's leading cryptographers, Professor Bart Preneel of KU Leuven, characteristically stated: "gradually all services on the internet at the European level will acquire an entry barrier, therefore the consequences will be enormous for everyone. […] If you want to get rid of anonymity on the internet, you must first put a 'door' on every service, because the internet currently has no 'doors'. So you start with one 'door' and with a state-controlled

application, and in the future it is not difficult for this application to be updated in a way that the identity [of the user] can be revealed."

Therefore, as access to services becomes dependent on prior identity verification through specific "entry gates," such as digital wallets in this case, this development may lead not only to a restriction of anonymity but also to a reconfiguration of the very architecture of the internet, with potentially far-reaching negative consequences for fundamental rights in the digital space.

In conclusion, the proposed regulation, although presented as a measure for the protection of children, raises broader issues concerning the institutional balance between security and freedom in the digital environment. The establishment of generalized age-verification mechanisms, without clearly defined safeguards and without demonstrated necessity in relation to less intrusive means, entails the risk of normalizing the elimination of anonymity on the internet.

(2) Non-transparent handling of the relevant recommendation of the competent committee of the Central Health Council (KESY)

Following a request from the Ministry of Health, the competent Mental Health Committee (ΕΨΥ) of the Central Health Council (KESY) appointed a four-member group of experts, chaired by the distinguished Dr Argyrios Stringaris, to formulate guidance regarding "the use of smartphones and social media by minors up to the age of 13." The expert group submitted a substantiated recommendation on 20 March 2026, which was unanimously approved by the ΕΨΥ and subsequently referred to the Plenary of KESY. However, the announcement of the measure on 8 April intervened abruptly, without any commentary on the arguments presented, or even a simple acknowledgment of the existence of the said recommendation. While such opinions are not binding on the government, in the present case it appears that they were not taken into account at all.

Dr Stringaris has summarized the conclusion of the recommendation in a relevant public post, stating that "instead of a blanket ban, it is preferable to place emphasis on targeted measures restricting minors' access to inappropriate content and on regulating providers' practices, as well as on educating young users, educators, and their families." The following point (3) makes specific reference to the content of this recommendation.

(3) Lack of participatory and evidence-based lawmaking

Unfortunately, the measure does not comply with the principle of participatory lawmaking, as it has not been accompanied by the involvement of citizens and stakeholders during the legislative drafting process, despite announcements by the Greek Government over the past year regarding the forthcoming legislative initiative and related press leaks.

In particular, according to publicly available information, no tools for gathering views, such as public consultations or questionnaires, have been utilized, nor have thematic meetings or consultations been organized with the participation of competent authorities, experts, academics, civil society, and children themselves, as is provided

for under Article 12 of the United Nations Convention on the Rights of the Child (Law 2101/1992, hereinafter "the Convention").

This Convention is binding on the Greek State, and under its provisions legislators are required to hear children and take their views into account before any administrative procedure affecting them. Relevant arguments are also set out by the United Nations Committee on the Rights of the Child in General Comment No. 25, entitled "Children's rights in relation to the digital environment" (paras. 16–18).

At this point, it should be emphasized that civil society organisations in Greece, such as Youth in the Loop and the Network for Children's Rights, have developed relevant tools, including targeted questionnaires and focus groups with children aged 10–15, within the framework of the national consultation campaign "Listen to us first. Our digital world." Furthermore, the experience of scientific bodies such as the Society for Regional Development and Mental Health, E.P.A.P.S.Y., derived from the operation of participatory structures, including the Youth Advisory Group within the 'It's up to Youth' programme, highlights the importance of the active involvement of adolescents themselves in the design of policies that concern them. Therefore, it is important for legislators, within this context, to adopt the principle: 'Nothing about adolescents without adolescents".

We underline that the corresponding parliamentary processes on this issue in the United Kingdom reflect a fundamentally different approach compared to the domestic one. Relevant regulatory initiatives are subject to continuous consultation. In the most recent phase of examining the issue of age restrictions, from January 2026, prior to the announcement of any legislative proposal, a multi-month, thorough, and transparent consultation process has taken place, with the participation of experts, civil society organisations, parents, and children. In this way, the full range of available options is examined from all perspectives, so as to ultimately arrive at the most well-substantiated and proportionate approach.

Furthermore, in the present legislative drafting process, the principle of evidence-based lawmaking is not respected. Specifically, the development and implementation of such a measure cannot be considered justified unless it is clearly demonstrated that the expected benefits substantially outweigh any potential harmful consequences. In this light, and insofar as the effective protection of users is sought, it is absolutely necessary to conduct a thorough and in-depth prior assessment of the risks and broader consequences of age-based controls before imposing them on a large-scale, online basis.

Undoubtedly, certain clinical and psychosocial findings concerning social media and its use by children should be emphasised. The first relates to emotional irritability and aggression. More specifically, although intensive engagement with social media may be associated with increased emotional irritability and manifestations of aggression among adolescents, it is crucial to emphasise that such characteristics do not lead in a linear or inevitable manner to delinquent or violent behaviour, but rather constitute risk factors interacting with the broader psychosocial context of each young person.

The second concerns disengagement from the educational process. In particular, it should be noted that, through the implementation of the psychosocial intervention

programme “It’s up to Youth” by E.P.A.P.S.Y., as well as through focus groups conducted by the same organisation with educators, a clear correlation has emerged between excessive use of social media and phenomena of adolescents becoming disengaged from the educational process.

Finally, the third concerns body image and the formation of children’s identity. More precisely, exposure to social media content may negatively affect adolescents’ body image by reinforcing unrealistic standards and social comparisons. At the same time, it has been observed that identity formation, including sensitive aspects such as sexual orientation and gender expression, is to a significant extent shifting into the digital environment, thereby requiring particular attention and sensitivity.

However, as discussed above (point 2), the only relevant expert recommendation from KESY appears not to have been taken into account at all. In particular, in an interview with journalist Eliza Triantafyllou for inside.story, Dr Stringaris notes that the recommendation provided a detailed analysis showing that the current consensus in the international literature is that, for the general population of children and adolescents, a causal link between social media use and mental health has not been sufficiently established.

He further explains that, according to the precautionary principle, legislators may adopt measures even where a causal link cannot be fully proven. However, at this point, the issue of proportionality arises, which is of particular importance in light of contemporary conditions, as we live in a digital era in which children are expected to become familiar with the digital world, which now constitutes an integral part of the public sphere. Consequently, the recommendation concluded that the imposition of blanket bans may lead to unforeseen and potentially adverse consequences for children. For this reason, the experts emphasized that developments in countries such as Australia should be carefully examined and that policymakers should await reliable data before making final decisions.

Therefore, the implementation of similar measures in other countries makes it even more imperative to carry out a systematic and empirically grounded assessment of both the benefits and the impacts of such technological interventions, rather than adopting them uncritically or prematurely in Greece. Indeed, in Australia, the most recent research data already raise concerns regarding the effectiveness of such regulatory approaches.

(4) Socio-economic exclusion and incompatibility with the principle of non-discrimination

Serious questions arise as to the implications that the use of age-verification applications may have in relation to the principle of non-discrimination. Existing age-verification methods generally presuppose the use of a modern “smart” mobile device, as well as the possession of adequate digital skills, particularly on the part of children’s parents. As a result, a reasonable question arises as to whether parents who do not possess such devices or lack the necessary digital skills will be able to comply with the measure in question.

Similarly, individuals who do not possess identity documents are unable to meet the requirements of most age-verification tools, with the result that they are excluded from access to basic means of communication with their relatives within the Greek territory. This situation may amount to indirect discrimination on the grounds of race, colour, ethnic or social origin, in violation of Article 21 of the Charter of Fundamental Rights of the European Union. Relevant arguments are also set out by the United Nations Committee on the Rights of the Child in General Comment No. 25, entitled "Children's rights in relation to the digital environment" (paras. 9–11).

(5) Disproportionate interference with the Rights of the Child

Age-based restrictions may constitute a disproportionate interference with the fundamental rights of children and, as such, may not be in compliance with international, national, and EU law.

Specifically, as expressly provided in Article 17(e) of the Convention on the Rights of the Child (hereinafter "the Convention"), which has been ratified by the Greek State (Law 2101/1992) and is legally binding upon it, States are required to "encourage the development of appropriate guidelines for the protection of the child from information and material injurious to his or her well-being, bearing in mind the provisions of Article 13," which guarantees the child's right to freedom of expression through any medium of their choice. Young people's freedom of information, expression and assembly nowadays is exercised to a great extent through online spaces and online tools, in a manner which cannot be replaced by 'offline' interactions.

Therefore, a restriction, such as the one proposed by the Greek Government, could be in conflict with Articles 13 and 15 of the Convention, as well as with Articles 11 and 12 of the Charter of Fundamental Rights of the European Union.

We further emphasize that, to the extent that such restrictions do not meet the requirements of necessity and proportionality, they also become incompatible with Article 24 of the Charter, which establishes the primacy of the best interests of the child, as reflected in Article 3 of the Convention, as well as with Article 12 of the Convention, which enshrines the child's right to freely express their views.

In this respect, the Hellenic National Youth Council (ESYN), which speaks on behalf of the Greek Youth, has already indicated through an open letter that the Greek youth reject their exclusion based on age verification. Young people prefer empowerment rather than control and top-down restrictions. The open letter signed by ESYN was also signed by organisations representing marginalised youth, such as LGBTQIA+, disabled, religious minorities and migrant communities. Through social media bans, these young people stand to lose not mere entertainment, but actual lifelines: networks where they find information, community, and support that may not exist elsewhere.

Relevant arguments are also set out by the United Nations Committee on the Rights of the Child in General Comment No. 25, entitled "Children's rights in relation to the digital environment" (paras. 50–66), while a comprehensive account of the various rights of child users directly affected by such legislative initiatives is also provided in a recent study by the European Union Agency for Fundamental Rights.

(6) Risk of displacement of children to non-compliant platforms and easy circumvention of measures through technical means

As argued by more than 400 academics and computer scientists from over 30 countries in a recent joint open letter, age-verification mechanisms can be easily circumvented, as demonstrated by existing applications that are bypassed through the use of virtual private networks (VPNs). In this way, child users may be exposed to additional risks.

As is well known, VPN providers that offer their services free of charge typically collect and process users' personal data in order to sell it to data brokers, which in turn leads to profiling and significant privacy challenges. Moreover, when a user employs a VPN to access a platform from a country outside the EU, they also lose important additional protections afforded by EU law for the protection of their personal data, among others.

Finally, as children may indeed seek to connect to lesser-known platforms in order to avoid age verification, they risk being exposed to malware and fraud. Furthermore, as also noted by the Greek CSO Network for Children's Rights in a relevant statement, children who circumvent such restrictions are particularly unlikely to report incidents they may encounter on those platforms, for fear of revealing their "irregular" presence.

(7) Unclear announcements regarding the proposed regulation, which hinder public debate and may create misleading impressions in relation to the proposed text of the Draft Law

Unfortunately, certain unclear, and even contradictory, statements have been identified regarding the proposed measure, which require further clarification, as they create misleading impressions in the public debate.

First, the Press Release (PR) of the Ministry of Health states, already in its opening paragraph, that "the draft bill under preparation introduces a clear and coherent framework for the protection of minors in the digital environment, fully aligned with European law and the guidelines of the European Union." However, in the very same PR publication, this time within the Q&A document, the Ministry of Health appears to contradict this statement, as it notes that "time is required to assess whether the proposed measure can be implemented without creating legal or operational conflicts with the European framework." This latter approach reflects reality, given that the applicable legal framework raises complex issues of compatibility (see point 8) and may create conditions of legal uncertainty in the context of compliance with existing EU legislation. This uncertainty may lead social media providers and other platform operators to seek the referral of preliminary questions to the Court of Justice of the European Union, potentially causing delays in the implementation of the measure, intensifying legal ambiguity, and resulting in insufficient practical protection for users. Moreover, these challenges also give rise to the obligation of the Hellenic State to publish the relevant Draft Law within the framework of the TRIS procedure on the relevant platform of the European Commission.

Second, under the proposed legislative initiative, "access to online social networking services is prohibited." EU law defines, in the Digital Markets Act (DMA), the concept of an "online social networking service" as "means a platform that enables end users to connect and communicate with each other, share content and discover other users and content across multiple devices and, in particular, via chats, posts, videos and recommendations." This definition is binding in nature, meaning that Member States, including Greece, cannot deviate from it. Contrary to press reports suggesting the existence of a closed and dynamic list of specific social media platforms to which the measure would apply (an approach that could raise additional compatibility issues with EU law), neither the Press Release nor the Ministry of Health's Q&A document contains any such official reference. The same approach is also reflected in the text of the Draft Law published by the Greek Government on the TRIS platform, as it is evident from proposed Articles 3 and 4 that the regulation applies horizontally to all providers of online social networking services, without distinction.

Consequently, if the measure is intended to have horizontal application across all social networking platforms, there is a possibility that it may indiscriminately encompass decentralized online platforms of the so-called Fediverse, such as Mastodon or PixelFed. These platforms operate under a different business and technological model compared to dominant social media services; they are not based on a central corporate structure and, as a rule, do not employ technical and design practices that promote addictive use.

In this light, their potential inclusion within the same regulatory framework as platforms such as TikTok, Facebook, Instagram, Snapchat, or X raises issues of proportionality and regulatory differentiation. At the same time, due to their decentralized nature (as they are not owned by a single legal entity but consist of numerous independent servers operated by distinct communities), significant practical challenges also arise with regard to the implementation and enforcement of the measure.

Furthermore, under the DMA, a "video-sharing platform service" is distinct from an "online social networking service," meaning that platforms such as YouTube do not qualify as social media services in the legal sense of the term. Consequently, the Greek Government has chosen not to include YouTube within the scope of the proposed regulation, a point also clarified by Mr Papastergiou during the press conference presenting the measure (in response to a question by journalist Mr Mallas from CNN Greece, from 52:00 onwards). The same approach is also followed in the Draft Law published on the TRIS platform. Since the measure, pursuant to Article 1 of the Draft Law, aims to protect mental health, it should be clarified why certain platforms are exempted and that decision should be justified on the basis of quantitative and qualitative data, which are absent from the announcements of the Hellenic State.

At this point, it is important to emphasize that both types of online platforms (i.e., both social networking services and video-sharing platforms) are subject to the obligations set out in Article 28 of the Digital Services Act (DSA), insofar as they are addressed to children. Indeed, Article 28 constitutes the core legal basis upon which the legislative initiative of the Greek State is built. Therefore, the decision to target social networking platforms, rather than video-sharing platforms, is a policy choice of the Greek Government, which requires further justification.

(8) Obligation to comply with the applicable EU legal framework

It is important to highlight that, unfortunately, there is a lack of clarity regarding both the content and the binding nature of the proposed measure. In particular, based both on the Press Release and the Q&A document published by the Ministry of Health, it was understood that, from January 2027, platforms will be required to proceed with a scenario of age re-verification of all accounts in Greece, so that accounts with a declared age different from the actual one and below the established thresholds will be excluded from the use of social media and will be required to undergo verification through a tool such as a "Kids Wallet." However, in statements made during the same press conference, Mr Papastergiou indicated that, ultimately, there will be no such obligation imposed on platforms to use the Kids Wallet (from 24:40 onwards and 49:17 onwards).

Ultimately, the Draft Law notified by the Greek Government to the European Commission on 8 May and published on the TRIS Platform on 12 May provides, in Article 4(3), that: "Providers of online platforms offering online social networking services shall implement appropriate, proportionate and reliable age-verification methods, including the equivalent European Union age-verification solution, which is integrated into the 'Gov.gr Wallet' application under Article 80 of Law 4954/2022 (Government Gazette A' 136) and into the 'Kids Wallet' application under Article 80A of Law 4954/2022, with the aim of restricting access to users who have not reached the age limit provided for in paragraph 1," namely 15 years of age. Furthermore, pursuant to paragraph 4 of the same Article: "Providers of online platforms offering online social networking services may complement age-verification techniques with age-estimation methods, where deemed necessary to ensure a high level of privacy, security and protection of minors." Therefore, it must first be assessed by the European Commission whether the proposed measure creates new obligations for platforms, or whether Article 4(3) merely restates the existing obligations arising from Article 28(1) and Article 35(1)(i) of the DSA. In any event, Article 4(4) does not create any actual obligation, since it contains the term "may" and therefore constitutes a proposed self-regulatory measure without any binding force.

It must be emphasized that, depending on the nature of the obligation, issues of compatibility with the Digital Services Act (DSA) may arise, as well as with Directive 2000/31/EC, which remains in full force alongside the provisions of the DSA, as interpreted by recent case law of the Court of Justice of the European Union (CJEU). Similar concerns have also been raised by legislators in other Member States, such as France and Germany, where comparable legislative initiatives are under discussion.

More specifically, the first compatibility challenge of the proposed national legislation concerns the very purpose of the DSA. As Recital 9 of the DSA expressly states, Member States should not adopt or maintain in force additional national requirements in matters falling within the scope of the Regulation, unless explicitly provided for, as this would undermine the direct and uniform application of the fully harmonised rules applicable to providers of intermediary services.

Accordingly, Member States are not permitted to adopt national provisions in areas of full harmonisation that pursue the same objectives as the DSA, since this would

undermine the direct and uniform application of the rules governing providers in the Digital Single Market. However, the legislative initiative of the Greek State is based on Article 28 DSA, without that provision expressly allowing Member States to introduce additional relevant national requirements. On the contrary, Article 28 of the DSA states that providers of online platforms are required to refrain from presenting advertisements based on profiling only where they have reasonable certainty that the recipient of the service is a minor. However, they are not required to process additional personal data in order to assess whether the recipient of the service is a minor, let alone under the age of 15, as envisaged by the proposed Greek regulation. Indeed, where platforms know, estimate, or have reasonable grounds to suspect that a user is under 18, they are required to take appropriate and proportionate measures to ensure a high level of protection. However, within this framework, age verification constitutes merely one of the indicative measures under Article 35 DSA and cannot, under any circumstances, constitute a standalone legal obligation for platforms, especially for the age of 15, as appears to be introduced by the proposed provisions of the Greek State on the basis of the Press Release, the published Q&A document and the Draft Law published on the TRIS platform. Therefore, if the measure is mandatory for platforms, Greece would be introducing additional national requirements in areas falling within the scope of the DSA Regulation, specifically Articles 28 and 35, thus conflicting with EU law.

Further elaborating, the core model of the DSA concerns the management of systemic risks rather than the prohibition of specific categories of users based on their age. In particular, platforms are required to carry out assessments in order to identify and mitigate systemic risks arising from their services (Articles 34–35), while at the same time ensuring a high level of protection of privacy, safety, and the protection of children (Article 28(1)). Indeed, this obligation is already being enforced by the Commission through preliminary findings concerning various social media platforms. Therefore, the imposition of an ex ante ban on the access of children under the age of 15 to social media platforms, through age verification, effectively removes the incentives for platforms to create safe environments for children and undermines both the enforcement of the DSA by the European Commission and the direct and uniform application of its fully harmonised rules.

The second compatibility challenge with EU law relates to Article 3 of Directive 2000/31/EC, which remains fully applicable. More specifically, under the country-of-origin principle provided for in that article, the Member State in which a provider of an information society service is established is responsible for the legality of its activity. Consequently, the activities of each platform, in addition to EU law, are governed by the law of the State in which it is established. Member States are required not to impose restrictions on information society services originating from another Member State, but rather to trust the national legal frameworks of other States and apply the principle of mutual recognition. Given that none of the platforms concerned by the proposed regulation are established in Greece, it could be argued that the adoption of the proposed national measure would violate both of these principles.

Admittedly, Directive 2000/31/EC provides for certain exceptions, under which Member States may adopt relevant legislative measures at national level. However, three cumulative conditions must be met for such measures: (1) they must be necessary for reasons of public policy, in particular the prevention, investigation, detection, and prosecution of criminal offences, including the protection of minors and the fight

against incitement to hatred on grounds of race, sex, religion, or nationality, as well as violations of human dignity concerning individual persons, or for the protection of public health, or for public security, including the safeguarding of national security and defence, or for the protection of consumers, including investors; (2) they must be directed against a specific information society service which prejudices the objectives referred to in point "(1)", or which constitutes a serious and grave risk of prejudice to those objectives; and (3) they must be proportionate to those objectives.

However, in the case of the proposed Greek national measure under consideration, these three criteria are not cumulatively fulfilled. In particular, the proposed measure does not satisfy criterion (1), as it primarily aims at safeguarding the well-being of minors and protecting them from technical and design practices that promote addictive behaviours. As such, it cannot be regarded as a necessary measure on grounds of public policy, particularly for the prevention or prosecution of offences for the protection of minors, or for the protection of public health, or for public security, including national security and defence, or for the protection of consumers, including investors.

With regard to the remaining criteria, the Court of Justice of the European Union has, through its settled case law, and in particular in its judgment in Case C-376/22, provided further interpretative guidance. In particular, even where criterion (1) is satisfied, the level of scrutiny applied remains particularly strict, including in relation to national measures aimed at addressing illegal online content. According to this case law, Member States may not impose general and abstract obligations on providers of information society services established in another Member State, as this would be contrary to the country-of-origin principle and would reintroduce restrictions on the free provision of services within the internal market.

The above compliance challenges are likely to prompt both the providers of social networking services to which the measure would apply, as well as other interested stakeholders, to seek the submission of preliminary questions before the Court of Justice of the European Union. Such a development may exacerbate legal uncertainty and undermine the effective practical protection of users.

Finally, it must be stressed that, within the EU legal order and in Greece, a legal framework already exists but is not adequately enforced. Since 2019 in Greece, through the implementation of Article 8 GDPR in Article 21 of Law 4624/2019, children under the age of 15 benefit from enhanced protection with regard to the processing of their personal data in the context of information society services where such processing is based on consent. However, in practice, large digital platform companies, since the entry into force of the GDPR (May 2018), have systematically sought to shift the legal basis for processing, opting for legitimate interest or the performance of a contract in order to circumvent the relevant protective obligations, thereby violating EU law. Similarly, the specific safeguards provided for in Article 28 of the Digital Services Act (DSA), concerning the protection of all minors (without differentiation by age group), remain limited and ineffective.

Instead of introducing new legislative measures, in its effort to strengthen the protection of children online, the Greek State could take a leading role in opposing the Digital Omnibus and Digital Omnibus on AI packages, which contain provisions that significantly weaken the framework for the protection of users in the digital

environment. We recall that the United States has made use of trade negotiations and, in particular, tariff measures as a means of influencing the regulatory policy of the European Union in the field of digital services and personal data protection, following pressure exerted by major technology companies based there.

(9) Cybersecurity challenges

Recent developments highlight that digital identity and age-verification applications are accompanied by significant cybersecurity challenges and technical vulnerabilities. Indicatively, just a few hours after the European Commission announced its new age-verification application, computer experts, speaking to POLITICO, raised a number of concerns regarding the design and the level of cybersecurity of the application, pointing to serious weaknesses and risks related to sensitive data breaches as well as identity theft.

A critical vulnerability was also recently identified in the Greek digital wallet application Gov.gr Wallet. Andronikos Koutroubelis, a graduate of the Department of Informatics at the Athens University of Economics and Business and co-founder of FactReview, notified the National Cybersecurity Authority immediately upon its discovery, as highlighted in a relevant report by inside.story and journalist Eliza Triantafyllou. The vulnerability existed from September 2025 until 22 April 2026, despite the competent authorities having been informed of the flaw as early as 30 March. It appears that it had escaped the controls of the system's owner, namely, the Ministry of Digital Governance and Artificial Intelligence, for more than six months. Both the identification of the vulnerability by an external third party and the delay in its remediation raise questions as to the nature of the security audits conducted, and by whom, on critical software deliverables within the Ministry.

At the same time, broader examples of data breaches in identity-verification systems demonstrate the heightened risks for the security and protection of users' personal data, as argued in a joint letter by more than 400 academics and computer scientists, to which reference has already been made above. The reliability of any security assessment presupposes the availability of the Kids Wallet source code under an open-source software regime and the possibility of review by bodies outside governmental authorities.

Therefore, prior to promoting the widespread, and in particular mandatory, use of such tools, a thorough and independent assessment of their security and reliability is necessary, in order to ensure that no new, systemic risks to citizens' rights are created.

(10) Need for a substantive emphasis on alternative solutions

Before concluding this letter, we consider it appropriate to highlight that strengthening education and digital literacy may constitute a suitable and proportionate alternative to horizontal restrictive measures. In particular, we consider it absolutely necessary to develop educational interventions within the school environment aimed at fostering digital literacy and critical thinking, a sense of responsibility and self-regulation, empathy and social skills, sexual education, and the mental resilience of children.

Equally critical is the provision of information, training and support to parents and parents' associations, so that they may develop the necessary skills to respond effectively to the challenges of the digital age.

Therefore, in this context, the development and implementation of targeted educational programmes, both within the school environment and at the family level, constitute a mild yet effective means of prevention with better long-term effects for the protection of individuals. In contrast, the proposed measure appears to lack such a multi-layered approach, which would include the education of children, as well as the promotion by the State of structured awareness-raising campaigns capable of strengthening children's critical judgment and meaningfully supporting parental guidance.

At the same time, the optimization and broader use of existing parental control mechanisms, such as a "Kids Wallet," could alternatively be considered, with a view to increasing their rate of adoption compared to current levels. Such mechanisms, when implemented with the consent and cooperation of children, enhance their protection while allowing restrictions to be tailored to their specific needs and level of maturity.

Nevertheless, it should be noted that their effectiveness presupposes that the online environment itself has been made less toxic, addictive and manipulative, and also presupposes access to appropriate "smart" devices and sufficient digital literacy, conditions that are not universally met, which may limit their practical applicability and create unequal conditions of protection.