



Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

TWENTIETH CONGRESS
Second Regular Session

HOUSE BILL NO. 10846



Introduced by Rep. ROBERT NAZAL

**AN ACT ESTABLISHING A MINIMUM AGE FOR SOCIAL MEDIA USE,
PRESCRIBING OBLIGATIONS FOR SOCIAL MEDIA PLATFORMS, PROVIDING
PENALTIES THEREFOR, AND FOR OTHER PURPOSES**

EXPLANATORY NOTE

Social media and digital platforms have become deeply embedded in the daily lives of Filipino children and young people. As of early 2025, the Philippines had approximately 97.5 million internet users, representing 83.8% of the country's population, while social media user identities reached approximately 90.8 million or around 78% of the population. Filipinos also remain among the world's heaviest internet users, spending an average of 8 hours and 52 minutes online daily.

While digital platforms provide opportunities for education, communication, entrepreneurship, creativity, civic participation, and access to information, they also expose minors to increasingly serious online harms. International child protection organizations such as UNICEF have documented how cyberbullying, online harassment, harmful content exposure, manipulative online behavior, and compulsive platform use can negatively affect the emotional, psychological, and social well-being of children and adolescents. UNICEF has likewise emphasized that cyberbullying may lead to anxiety, emotional distress, social withdrawal, loss of motivation, and mental health consequences among children and young people.

Today, digital platforms are no longer merely passive communication tools. Many social media systems are intentionally designed to maximize engagement through algorithmic amplification, personalized feeds, behavioral targeting, notifications, and continuous content exposure. These systems increasingly shape how children consume information, interact socially, and form opinions, often at ages where they may not yet possess sufficient maturity, discernment, or emotional resilience to safely navigate online risks.

This proposed “Children’s Safety in Social Media Act” seeks to establish a minimum age requirement of sixteen (16) years for the use of age-restricted social media platforms and to impose enforceable obligations upon platform providers to adopt reasonable, effective, proportionate, and privacy-preserving safeguards against underage access and harmful online exposure.

The measure adopts a rights-based and risk-based regulatory framework that balances child protection, constitutional freedoms, privacy rights, and access to information. Instead of placing the burden solely upon parents, guardians, or schools, the bill places primary responsibility upon covered social media platform providers to implement age assurance mechanisms and safety-by-design measures proportionate to the risks posed by their platforms.

The bill further recognizes the importance of protecting privacy and preventing excessive data collection. Accordingly, it prohibits the mandatory use of government-issued identification as the sole method for age verification and requires compliance with Republic Act No. 10173, otherwise known as the “Data Privacy Act of 2012.” It likewise mandates data minimization, purpose limitation, and safeguards against the unauthorized use or retention of personal information collected for age assurance purposes.

The measure also promotes digital citizenship, media literacy, and public awareness programs involving the Department of Information and Communications Technology (DICT), Department of Education (DepEd), National Privacy Commission (NPC), National Telecommunications Commission (NTC), Department of Social Welfare and Development (DSWD), Department of Justice (DOJ), Commission on Human Rights (CHR), and other relevant agencies. The bill recognizes that effective child online protection requires a whole-of-government and whole-of-society approach involving families, schools, communities, regulators, and technology platforms themselves.

The bill additionally establishes mechanisms for disabling underage accounts, reporting violations, implementing platform accountability measures, and enforcing administrative penalties for non-compliance. These provisions seek to ensure that online child safety obligations are enforceable, proportionate, and consistent with due process and constitutional protections.

Globally, governments have increasingly moved toward stronger online child protection frameworks. Australia enacted legislation in 2024 restricting social media access for children below sixteen (16) years old, reflecting growing international concern regarding the impact of social media platforms upon minors. Similar global policy discussions continue in various jurisdictions concerning age assurance, child online safety, platform accountability, and digital well-being.

This proposed measure likewise aligns with the constitutional duty of the State to defend the right of children to assistance, including proper care and special protection from all forms of neglect, abuse, cruelty, exploitation, and conditions prejudicial to their development.

It bears emphasizing that a substantially similar measure was already passed on Third Reading in the Senate during the 19th Congress through Senate Bill No. 1955 principally authored by Senator Loren Legarda.

In view of the foregoing, the swift passage of this measure is earnestly sought.



ROBERT NAZAL
Representative

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

TWENTIETH CONGRESS
Second Regular Session

HOUSE BILL NO. 10846

Introduced by Rep. ROBERT NAZAL

**AN ACT ESTABLISHING A MINIMUM AGE FOR SOCIAL MEDIA USE,
PRESCRIBING OBLIGATIONS FOR SOCIAL MEDIA PLATFORMS, PROVIDING
PENALTIES THEREFOR, AND FOR OTHER PURPOSES**

*Be it enacted by the Senate and House of Representatives of the Philippines
in Congress assembled:*

Section 1. Short Title. – This Act shall be known as the “Children’s Safety in Social Media Act”.

Sec. 2. Declaration of Policy. – It is hereby declared the policy of the State to uphold the best interests of the child and to promote and protect the physical, mental, moral, spiritual, intellectual, and social well-being of children and the youth, consistent with the Constitution and the State’s obligations under the United Nations Convention on the Rights of the Child and other relevant laws.

Recognizing that digital platforms and social media have become integral to learning, communication, civic participation, creativity, and community life, the State shall protect children in the digital environment, while safeguarding their rights to freedom of expression, access to age- and developmentally-appropriate information, privacy, and the confidentiality of personal data.

In view of the demonstrated risks of harm arising from certain social media platform features and practices, including cyberbullying, sexual exploitation and abuse, exposure to harmful or age-inappropriate content, harassment, manipulation through design and algorithmic amplification, and patterns of compulsive or addictive use, the State adopts a risk-based and proportionate regulatory framework that focuses on preventing and reducing such harms without unduly restricting lawful speech, legitimate educational use, and beneficial online engagement.

To this end, the State shall place primary responsibility on covered social media platform providers, consistent with their public impact and duty of care, to implement reasonable, effective, and privacy-preserving measures to prevent children below the minimum age set by law from creating or maintaining accounts on covered platforms, subject to clear standards, regulatory guidance, and enforcement mechanisms.

The State shall ensure that any age-assurance or compliance measure is implemented in a manner that: (a) upholds data minimization and purpose limitation; (b) prevents the overcollection, commercial use, or retention of information gathered for age-assurance; (c) avoids compelling the use of government-issued identification or digital identification as the sole means of compliance; and (d) provides accessible safeguards and remedies against misuse, consistent with due process and the right to privacy.

The State further recognizes the primary right and duty of parents and guardians in the upbringing of children and shall support parental authority through accessible tools, transparency, and education, including media and digital literacy initiatives, while promoting whole-of-government coordination to ensure coherence with existing laws, child protection systems, cybercrime enforcement, education policies, and data privacy regulations.

Sec. 3. *Definition of Terms.* – For the purposes of this Act, the following terms are defined as follows:

(a) Account refers to a registered profile, username, or credentialed access that enables a user to log in to a platform and use features available to account holders, including posting content, reacting, messaging within the platform, participating in groups or channels, live streaming, receiving personalized recommendations, or receiving notifications tied to the user profile;

(b) Age Assurance refers to measures or methods reasonably designed to determine whether a prospective or existing account holder is an age-restricted user, which may include age estimation, age verification, age inference, parental or guardian attestation, or other privacy-preserving techniques, subject to this Act and applicable data protection laws;

(c) Age-Restricted User refers to a child who has not reached the minimum age specified in this Act for holding an account on an age-restricted social media platform;

(d) Age-Restricted Social Media Platform refers to an internet-based service, network, application, website, or computer program that satisfies all of the following conditions:

(1) The sole purpose, or a significant purpose, of the service is to enable online social interaction between two (2) or more end-users, including interaction that enables end-users to share material for social purposes;

(2) The service allows end-users to link to, communicate with, or otherwise interact with some or all other end-users; and

(3) The service allows end-users to post, upload, share, or otherwise make available user-generated content on the service; Provided, That “online social interaction” does not include primarily online business interaction in marketplaces, e-commerce, or service booking platforms.

(e) Child refers to any person below eighteen (18) years of age;

(f) Data Minimization and Purpose Limitation refer to the principles that information collected for age assurance and compliance shall be limited to what is necessary, used only for the permitted purpose, and retained only for as long as necessary to achieve that purpose.

(g) Disabling Order refers to a written order issued by the Department of Information and Communications Technology (DICT) directing a Social Media Platform Provider to disable, deactivate, or restrict access to an identified account or page pursuant to this Act.

(h) Excluded Services refer to online services, applications, websites, or platform features that would otherwise fall within the definition of an Age-Restricted Social Media Platform but are excluded from the minimum-age account restriction under Section 4 because they are low-risk and necessary for a child’s access to essential communications, education, health, safety, or public services, as determined under this Act and its Implementing Rules and Regulations (IRR).

A service or feature shall be considered an Excluded Service only if it meets all of the following criteria:

(1) Its primary purpose is to provide direct, limited-scope utility (e.g., messaging, learning, health/safety support, or delivery of government services), and not to provide a general-purpose feed-based environment for public social networking;

(2) It does not primarily rely on engagement-optimizing design that materially increases child-risk, including but not limited to algorithmic amplification to broad audiences, public follower networks by default, or open discoverability of minors; and

(3) Access and use can be provided in a manner consistent with data minimization, purpose limitation, and limited retention for child users.

Excluded Services include, but are not limited to:

(i) Interpersonal communications services, where communications are primarily one-to-one or closed-group and not publicly discoverable by default;

(ii) Education and learning management services, including school-authorized platforms used for instruction, assessment, official class communications, or school safety announcements;

(iii) Health, mental health, counseling, hotline, and safety-support services, including crisis lines and child-protection reporting channels;

(iv) Government digital services and official citizen service portals; and

(v) Other services or features that the DICT, in consultation with the National Privacy Commission (NPC) and the National Telecommunications Commission (NTC), may classify by IRR as excluded, based on a documented finding that the service is low-risk and necessary, consistent with the best interests of the child and the child's right to useful, meaningful, and safe access to digital technologies.

(i) Government-Issued Identification refers to any identification document or credential issued by the Philippine government or any of its instrumentalities, including any digital identification system recognized by the State, as may be defined by law.

(j) Internet Service Provider (ISP) refers to any public telecommunications entity (PTE) or value-added service provider duly authorized by or registered with the National Telecommunications Commission (NTC) that provides users or other entities with data connection allowing access to the internet through physical transport infrastructure, and such access is necessary for end-users to access online content and services and for content providers or platform providers to publish, host, or distribute materials online.

(k) Personal Data refers to any information, whether recorded in material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained, or when put together with other information would directly and certainly identify an individual, consistent with applicable laws.

(l) Reasonable Steps refers to objectively appropriate, effective, and proportionate measures that a Social Media Platform Provider is expected to adopt to comply with this Act, taking into account available technologies, efficacy, risks of circumvention, the scale and nature of the platform, implementation cost relative to platform capacity, impacts on privacy, and the best interests of the child.

(m) Service Provider refers to any natural or juridical person, whether domestic or foreign, that, in connection with an Age-Restricted Social Media Platform or the implementation of this Act, provides, operates, controls, or enables any of the following: (a) the platform or any component thereof; (b) hosting, content delivery, caching, domain name services, or other network services; (c) app distribution or access facilitation; or (d) internet access or connectivity services; and includes a Social Media Platform Provider and an Internet Service Provider.

(n) Social Media Platform Provider refers to any natural or juridical person, whether domestic or foreign, that owns, operates, controls, or makes available an age-restricted social media platform in the Philippines, including through an app or web-based interface, and determines the purposes and means of processing user data for such platform.

(o) Third-Party Age Assurance Provider refers to any natural or juridical person, whether domestic or foreign, that provides, operates, or supplies age verification or age assurance systems, services, software, tools, or application programming interfaces (APIs) to a Social Media Platform Provider for purposes of determining whether an individual is an Age-Restricted User, and that processes Personal Data for such purpose, whether as an independent entity or as a processor engaged by the Social Media Platform Provider.

Sec. 4. *Minimum Age Restriction for Social Media Accounts.* – A child who has not reached sixteen (16) years of age shall be an age-restricted user and shall be prohibited from holding, creating, or maintaining an account on an age-restricted social media platform.

For the avoidance of doubt, the minimum age restriction under this Act applies solely to the creation, holding, or maintenance of an account on an age-restricted social media platform and account-based interactive participation therein.

Provided, That the restriction under this Section shall not apply to electronic services, platforms, or platform features deemed as Excluded Services as defined in this Act.

Nothing in this Act shall be construed to prohibit passive viewing of publicly available content where no account registration or login is required, subject to existing child protection laws that apply irrespective of login state.

Sec. 5. *Obligation of Social Media Platform Providers.* – The provider of an age-restricted social media platform shall take reasonable steps to prevent age-restricted users from registering, accessing, holding, or continuing to use accounts on the platform.

Reasonable steps shall include, at a minimum, measures reasonably designed to address:

- (a) New account creation (e.g., registration and onboarding);
- (b) Existing accounts (e.g., review, restriction, deactivation/removal, as appropriate); and
- (c) Circumvention risks (repeated evasion attempts and abuse of verification processes).

In determining whether steps are reasonable, regard shall be had to:

- (a) The nature and size of the platform and the risks posed to children;
- (b) The effectiveness and proportionality of the measures adopted;
- (c) The privacy impacts of age assurance and the availability of less intrusive options; and
- (d) The need to avoid measures that unduly impair lawful communication, education, and participation.

Social Media Platform Provider shall maintain documented policies, procedures, and technical measures adopted to comply with this Act, and shall keep compliance records sufficient for verification by the DICT, consistent with data minimization and purpose limitation. Such records shall be limited to what is necessary to demonstrate compliance and shall not require the retention of personal data beyond what is permitted under Section 9 of this Act.

Social Media Platform Providers shall submit to the DICT, at such intervals and in such form as may be provided in the IRR, an aggregated compliance report describing the reasonable steps undertaken, implementation status, and effectiveness indicators, without disclosing personal data except to the extent strictly necessary for regulatory verification and consistent with the Data Privacy Act.

Sec. 6. *Age Assurance Measures.* – For purposes of complying with the minimum age obligation, a Social Media Platform Provider may adopt age assurance measures that are reliable, proportionate, and privacy-preserving, and are designed to prevent age-restricted users from registering for, accessing, or continuing to use the platform. Such measures may include, as applicable, account-based signals, user interaction-based methods, third-party age assurance services, or other measures permitted under rules issued pursuant to this Act.

To prevent overcollection of sensitive identity data, a Social Media Platform Provider shall not require government-issued identification, or any government or government-accredited digital identity system, as the sole means for an individual to demonstrate that the individual is not an age-restricted user. Where government-issued identification is offered as an option, the Social Media Platform Provider must make available at least one reasonable alternative.

Sec. 7. *Digital Well-Being and Break Tools.* – Social Media Platform Providers shall make available to all users, and in a manner that is privacy-preserving and easy to use, digital well-being controls that enable: (a) voluntary time limits and scheduled “quiet hour”; (b) break reminders and notification management; and (c) for accounts reasonably determined to be used by minors, parent- or guardian-controlled scheduling tools, subject to safeguards in this Act.

No user shall be penalized solely for declining to enable such tools. The DICT shall issue guidance standards in consultation with the NPC to ensure data minimization and to prevent the collection of additional personal data solely for implementing these tools.

Sec. 8. *Safety-by-Design for Permitted Child Use.* – Where: (a) a child is permitted to use an Excluded Service under this Act or its implementing rules and regulations, or (b) a child who is not age-restricted and is permitted to hold an account on a social media platform, the Social Media Platform Provider of such service or platform shall implement and maintain age-appropriate default settings and safety measures for such child users.

At a minimum, such measures shall include:

(a) Applying privacy-protective defaults, including limiting profile visibility and restricting geolocation sharing, searchability, and direct messaging from unknown users, where applicable;

(b) Providing accessible parental guidance tools, including features that enable parents or legal guardians, where applicable and voluntarily enabled, to supervise settings, manage contacts, and set reasonable time or usage controls, without requiring the disclosure of additional personal data beyond what is necessary;

(c) Maintaining clear and child-sensitive reporting and response mechanisms for harmful content, harmful contact, and misuse, including acknowledgement and timely action consistent with the implementing rules;

(d) Implementing measures reasonably designed to reduce exposure to age-inappropriate content, including content labeling, filtering options, and age-appropriate recommendations where such systems are used; and

(e) Ensuring transparency, through plain-language notices on applicable child safety settings and how to access or modify them.

Nothing in this Section shall be construed to authorize restrictions on lawful participation, access to information, or expression except to the extent necessary, reasonable, and proportionate to protect the best interests of the child and to carry out the purposes of this Act, consistent with the Constitution.

Sec. 9. *Data Privacy.* – Any personal data collected or processed for purposes of following compliance with the minimum age obligation shall be subject to the following:

(a) Collecting only what is strictly necessary to determine whether an individual is an age-restricted user;

(b) Using or disclosing the data solely for age assurance and enforcement of this Act, and for no other purpose;

(c) Applying appropriate organizational, physical, and technical security measures, including encryption and access controls;

(d) Destroying or irreversibly de-identifying the data as soon as it has served the purpose for which it was collected, unless retention is required by law; and

(e) Complying with Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012 and all other applicable data protection laws, rules and regulations.

Violation of this provision shall be subject to penalties under this Act, the Data Privacy Act of 2012, and any other administrative, civil or criminal penalties as may be prescribed by law.

Sec. 10. *Account Audits, Deactivation, Anti-Circumvention, and Reporting.* – Social Media Platform Providers shall:

- (a) Conduct risk-based audits of accounts and signals reasonably indicative of age misrepresentation, and deactivate accounts of age-restricted users;
- (b) Mitigate circumvention by preventing reactivation or creation of duplicate accounts by previously deactivated age-restricted users, consistent with privacy safeguards;
- (c) Provide a readily accessible reporting mechanism for users and parents/guardians to report suspected age-restricted accounts; and
- (d) Adopt prompt, documented response procedures for reports and findings under this Act.

Sec. 11. *Role of the Department of Information and Communications Technology.* – The DICT shall be the primary implementing and coordinating agency for the enforcement of this Act in relation to platform compliance with the minimum age obligation and related safety duties, without prejudice to the mandates of the NPC under Republic Act No. 10173, the NTC, and other concerned agencies. In carrying out this Act, the DICT shall exercise the following powers and functions:

- (a) Monitoring compliance of Social Media Platform Providers and, where applicable, Third-Party Age Assurance Providers, with age restrictions and related duties under this Act;
- (b) Receiving and maintaining accessible reporting channels for suspected violations, including underage access, circumvention, and platform non-compliance;
- (c) Investigating alleged violations, *motu proprio* or upon complaint, and conducting compliance checks consistent with due process and data minimization;
- (d) Issuing compliance notices requiring Social Media Platform Providers to take specified actions within a stated period, including removing, suspending, or restricting accounts reasonably determined to be held by age-restricted users, and reporting back the steps taken;

(e) Referring matters involving privacy or personal data processing to the NPC for appropriate action, and coordinating with the Office of Cybercrime of the Department of Justice (DOJ) and other law-enforcement agencies for criminal violations;

(f) Coordinating with the NTC, DepEd, DSWD, CHR, and other relevant agencies to ensure child-sensitive, rights-respecting, and technically workable implementation, including on education-related access where expressly allowed by this Act;

(g) Recommending and supporting the issuance of implementing rules and technical standards, including age assurance guidance, in coordination with the NPC and other agencies concerned; and

(h) Requiring Social Media Platform Providers and, where applicable, Third-Party Age Assurance Providers to submit documented compliance policies, technical descriptions, aggregated compliance reports, and to produce compliance records necessary to verify adherence to this Act, subject to data minimization, purpose limitation, and applicable privacy safeguards.

Sec. 12. Inter-Agency Council on Children's Safety in Social Media. – There is hereby created an Inter-Agency Council on Children's Safety in Social Media (the Council) to ensure a coordinated, rights-respecting, and technically workable implementation of this Act.

The Council shall be composed of the following ex officio members:

(a) The Secretary of the Department of Information and Communications Technology (DICT), who shall serve as Chairperson.

(b) The Commissioner of the National Privacy Commission (NPC), who shall serve as Vice-Chairperson.

(c) The Chairperson of the NTC, who shall serve as Member.

(d) The Secretary of the Department of Education (DepEd), who shall serve as Member.

(e) The Secretary of the Department of Social Welfare and Development (DSWD), who shall serve as Member.

(f) The Secretary of the Department of Justice (DOJ), through the Office of Cybercrime, who shall serve as Member.

(g) The Chairperson of the Council for the Welfare of Children (CWC), who shall serve as Member.

(h) The Chairperson of the Commission on Human Rights (CHR), who shall serve as Member.

(i) One (1) representative from the National Youth Commission (NYC), who shall serve as Member.

Such other heads of agencies as may be designated in the IRR, consistent with their respective statutory mandates, who shall serve as Members for purposes of carrying out specific functions under this Act.

Each member-agency may designate a permanent alternate representative, who shall not be lower than an Assistant Secretary or its equivalent, and who shall have full authority to act and vote on behalf of the principal.

The DICT shall serve as Secretariat of the Council.

The Council may invite, as non-voting resource persons, representatives from relevant stakeholders, including Social Media Platform Providers, civil society, academe, mental health professionals, and child-rights organizations, as may be necessary in the performance of its functions.

Sec. 13. *Public Awareness and Digital Well-Being Programs.* – The DICT shall, in coordination with the Philippine Information Agency (PIA) and in consultation with the DepEd, Department of Health (DOH), NYC, the NPC, local government units, and other relevant agencies, the private sector, and civil society organizations, develop, lead, undertake, and coordinate a nationwide program to heighten public awareness, parental empowerment, and community involvement in furtherance of the purposes of this Act.

For this purpose, the DICT shall implement a sustained information and education campaign, which shall include:

(a) Promoting internet safety and child online protection best practices, including practical guidance on privacy settings, reporting tools, content controls, and safe-by-design use of platforms;

(b) Conducting a national outreach and education campaign through broadcast, print, community-based activities, and online resources, to inform the public of online risks to children, including cyberbullying, exploitation, harmful content exposure, and excessive or compulsive use;

(c) Facilitating access to updated information and resources on online safety, child development, and age-appropriate digital use, including materials for parents, guardians, educators, and learners;

(d) Coordinating with DepEd and DOH on school- and community-based interventions to address digital overuse and its links to mental and physical health, including awareness of warning signs, healthy screen habits, and pathways for referral and support; and

(e) Strengthening public confidence in child online protection measures by ensuring that public advisories and education materials emphasize proportionate safeguards, parental tools, and privacy-preserving practices consistent with applicable data protection laws and regulations.

Sec. 14. *Digital Citizenship Literacy.* – The DepEd shall ensure that the K to 12 curriculum is supported by age-appropriate programs on digital citizenship and media and information literacy, including online safety, critical thinking, responsible expression, and reporting mechanisms, consistent with Republic Act No. 10533 or the Enhanced Basic Education Act of 2013. The Commission on Higher Education (CHED) and the Technical Education and Skills Development Authority (TESDA) shall likewise promote and integrate digital citizenship literacy programs, as applicable, within their respective mandates.

Sec. 15. *Online Safety Coordinators.* – There shall be appointed an Online Safety Coordinator (OSC) in all primary and secondary schools. They shall ensure the protection of all students from potential harms that may occur through the internet and electronic media and serve as the main contact person on all online-related issues. OSCs shall act as auditor of online safety measures, including the collection and safe handling of safety incidents.

Sec. 16. *Disabling of Age-Restricted Accounts.* – When the DICT, upon prima facie determination based on verified information or complaint, finds that an account or page is owned, controlled, or principally used by an Age-Restricted User, it shall issue a Disabling Order directing the relevant Social Media Platform Provider to disable, deactivate, or restrict access to the identified account or page within forty-eight (48) hours from receipt of the Order.

The Disabling Order shall be implemented in a manner that is necessary and proportionate, and limited to what is required to enforce the minimum age restriction, consistent with constitutional protections on expression and due process.

Within twenty-four (24) hours from issuance of the Disabling Order, the DICT shall furnish the NTC a copy thereof and indicate the date and time of service upon the Social Media Platform Provider, for purposes of monitoring compliance by Social Media Platform Providers and, where applicable, coordinating action within its jurisdiction pursuant to this Act and other applicable laws.

The Social Media Platform Provider shall document implementation of the Disabling Order and, within three (3) days from implementation, shall submit to the DICT and furnish the NTC a compliance report stating: (a) the action taken and the date and time of implementation; (b) the steps undertaken to prevent reactivation or circumvention of the disabled account consistent with this Act; and (c) the notification made under this Act and its implementing rules: Provided, That the report shall not include Personal Data beyond what is strictly necessary for regulatory verification, consistent with the Data Privacy Act and the principles of data minimization and purpose limitation.

Sec. 17. *Request to Lift Disabling Order.* – The Social Media Platform Provider may provide an accessible mechanism for the account owner and, where applicable, the parent or legal guardian, to request the lifting or modification of a Disabling Order on the ground of erroneous age classification. The request shall include supporting information sufficient to reasonably establish that the account holder is not an Age-Restricted User, consistent with this Act, the Data Privacy Act, and the IRR.

Upon receipt of the request, the Social Media Platform Provider shall transmit the request and relevant information to the DICT within three (3) days, together with a brief statement of the basis for the Disabling Order and the platform's relevant age assurance indicators, limited to what is necessary for review.

The DICT shall resolve the request within ten (10) days from receipt based on substantial evidence, and shall either: (a) affirm the Disabling Order; or (b) direct the lifting or modification of the Disabling Order and the restoration of access, in whole or in part, subject to appropriate safeguards consistent with this Act. Pending resolution, the disabling or restriction shall remain in effect.

Where the DICT directs restoration, the Social Media Platform Provider shall restore access within forty-eight (48) hours from receipt of the DICT directive.

Sec. 18. *Compliance of Service Providers.* – Service Providers, including Social Media Platform Providers and, where applicable, Internet Service Providers, shall comply with a Disabling Order issued under Section 16 within forty-eight (48) hours from receipt.

If the Social Media Platform Provider fails or refuses to comply within the period, and after notice of such noncompliance, the DICT may recommend that the NTC require the implementation of effective and proportionate technical measures, as a measure of last resort, to prevent access to the specific account or page identified in the Disabling Order, subject to rules that minimize collateral blocking under the IRR.

Such technical measures may include:

- (a) Domain name blocking (DNS blocking) for the specific prohibited account/page access point;
- (b) URL blocking for the specific prohibited account/page address;
- (c) IP address blocking, only where strictly necessary and technically appropriate; and
- (d) Other functionally equivalent measures that are targeted, time-bound, and least restrictive.

Failure to comply with a Disabling Order, without lawful excuse, shall subject the responsible entity to the administrative penalties provided under this Act and other applicable laws, including: (a) the restriction, suspension, or prohibition of access to or operations of the covered service within the Philippines to the extent authorized under this Act; and (b) where the responsible entity holds a permit, license, franchise, certificate, or registration issued by another government agency, the DICT may recommend to the appropriate regulatory agency the suspension, cancellation, or appropriate action on such authorization.

Sec. 19. Penalties. – Any Social Media Platform Provider, or Third-Party Age Assurance Providers, that fails to comply with any provision of this Act, including but not limited to the failure to implement adequate Age Assurance measures, refusal to comply with a Disabling Order, unauthorized retention or misuse of personal data collected under this Act, shall be subject to the following administrative penalties, without prejudice to any civil or criminal liability under existing laws:

(a) For Social Media Platform Providers:

- (i) Fines of not less than One Million Pesos (Php 1,000,000) but not exceeding Twenty Million Pesos (Php 20,000,000) for each act of non-compliance, depending on the gravity and frequency of the violation;
- (ii) Daily fines of not more than One Hundred Thousand Pesos (Php 100,000) for each day of continuing violation after due notice; and

(iii) Suspension or revocation of access, operations, or licenses within the Philippines upon a finding of gross negligence, repeated non-compliance, or willful violation, subject to due process.

(b) For Third-Party Age Assurance Providers:

(i) Fines of not less than Five Hundred Thousand Pesos (Php 500,000.00) but not more than Five Million Pesos (Php 5,000,000) for breach of data privacy provisions or failure to meet verification standards set under this Act; and

(ii) Permanent disqualification from providing related services to social media platforms operating in the Philippines upon a finding of gross negligence, repeated non-compliance, or willful misconduct, subject to due process.

The imposition of the above penalties shall be without prejudice to prosecution under Republic Act No. 10173, otherwise known as the “Data Privacy Act of 2012”, Republic Act No. 10175, otherwise known as the “Cybercrime Prevention Act of 2012,” or any other applicable penal law.

Sec. 20. Appropriations. – The amount necessary to carry out the provisions of this Act is hereby authorized to be appropriated in the General Appropriations Act of the year following its enactment into law and thereafter.

Sec. 21. Implementing Rules and Regulations. – Within ninety (90) days from effectivity of this Act, the DICT, in consultation with the NTC, NPC, DOJ, DSWD, CHR, DepEd, DOH, and other appropriate government agencies, and after consultation with relevant stakeholders from the education, child protection, youth, and technology sectors, shall promulgate the necessary rules and regulations for the effective implementation of this Act.

Sec. 22. Separability Clause. – If any provision of this Act is declared unconstitutional or invalid, the remaining provisions shall remain in full force and effect.

Sec. 23. Repealing Clause. – All laws, decrees, executive orders, rules and regulations, or parts thereof inconsistent with this Act are hereby repealed or amended accordingly.

Sec. 24. Effectivity Clause. – This Act shall take effect fifteen (15) days after its publication in the Official Gazette or in a newspaper of general circulation.

Approved.