



Republic of the Philippines
House of Representatives
Quezon City, Metro Manila

Twentieth Congress
Second Regular Session

HOUSE BILL NO. 10743



Introduced by **REPRESENTATIVE KATRINA REIKO CHUA - TAI**

EXPLANATORY NOTE

The Constitution mandates the State to protect and promote the rights and welfare of children. This responsibility must likewise extend to the digital spaces where children increasingly learn, communicate, socialize, and express themselves.

Social media opens doors to learning and connection. Yet, it also leaves children vulnerable to cyberbullying, online exploitation and grooming, harmful content, privacy breaches, targeted ads, excessive screen time, and the hidden dangers of algorithm-driven feeds.

Existing laws offer some protection, but a more comprehensive framework is needed to clearly define the duties of social media platforms in safeguarding minors.

This bill introduces a framework that is mindful of risks, sensitive to age, and protective of privacy. It strengthens safeguards for young children, encourages meaningful parental involvement, and boosts privacy and safety for adolescents.

It also requires privacy-preserving age assurance consistent with the principles advanced by the National Privacy Commission. Age assurance should be proportionate to the risks involved, transparent and understandable to children, and subject to established data privacy principles. The NPC has likewise recognized that self-declaration alone may not be sufficient where the processing of children's personal data presents heightened risks.

The bill aims to reinforce age assurance in a way that avoids intrusive identity checks or sweeping surveillance, striking a careful balance between safety and privacy. The measure acknowledges that age restrictions alone cannot shield children from online dangers. Social media platforms must take responsibility for the environments they create. That is why the bill calls for default privacy and safety settings, robust parental controls, limits on behavioral profiling and targeted ads, protections against grooming and harmful content, responsible recommendation systems, greater transparency, and easy-to-use reporting and redress channels.

This approach builds upon the direction already emerging from the House of Representatives. House Bill No. 9965, for instance, incorporates age verification, parental

controls, privacy protections, algorithmic safeguards, transparency, digital literacy, and substantial penalties for violations. The present measure advances these principles within a unified framework that gives equal importance to child safety and data privacy.

Protecting children online is not a burden that should fall only on children or their parents. The platforms shaping these digital worlds must act with care and face consequences if they neglect the safeguards set by law.

The measure ultimately seeks to ensure that children can benefit from technology while being protected from the risks that accompany it. It recognizes that protecting children in the digital age requires not only appropriate age restrictions, but also responsible platforms, meaningful privacy protections, and enforceable safety standards.

In view of the foregoing, the immediate passage of this bill is earnestly sought.

A handwritten signature in black ink, appearing to read 'Katrina', with a stylized flourish extending from the end.

KATRINA REIKO CHUA-TAI

1 Nothing in this Act shall be construed to unduly restrict a child's rights to education,
2 information, communication, expression, privacy, association, or participation in matters affecting
3 the child.

4 SEC. 3. **Objectives.** – This Act shall have the following objectives:

- 5 (a) Establish minimum age-based rules for access to covered social media platforms;
- 6 (b) Require social media platforms to adopt reasonable and privacy-preserving age-
7 assurance mechanisms;
- 8 (c) Require stronger safeguards for child users;
- 9 (d) Protect children's personal and sensitive personal information;
- 10 (e) Prevent social media platforms from designing or operating systems that exploit the
11 developmental vulnerabilities of children;
- 12 (f) Strengthen parental and guardian tools without converting parents into permanent
13 monitors of their children's private communications;
- 14 (g) establish accountability and penalties for platforms that fail to comply with their
15 statutory duties;
- 16 (h) establish mechanisms for reporting, investigation, redress, and enforcement;
- 17 (i) promote digital literacy, responsible technology use, and healthy online behavior;
18 and
- 19 (j) ensure that regulation of children's social media use remains consistent with the
20 Constitution, the Data Privacy Act of 2012, the Anti-Child Pornography Act, the
21 Anti-Photo and Video Voyeurism Act, the Anti-Bullying Act, the Special
22 Protection of Children Against Abuse, Exploitation and Discrimination Act, the
23 Anti-OSAEC and CSAEM Act, and other applicable laws.

24 SEC. 4. **Definition of Terms.** – For purposes of this Act:

1 (a) "Age assurance" refers to the process by which a covered platform determines or
2 estimates, with an appropriate degree of reliability and proportionality, whether a
3 user falls within a specified age range.

4 (b) "Child" or "minor" refers to any person below eighteen (18) years of age.

5 (c) "Covered platform" or "social media platform" refers to an online service primarily
6 designed to enable users to create, share, disseminate, discover, recommend, or
7 interact with user-generated content or with other users through social networking,
8 social communication, public posting, content sharing, or substantially similar
9 functions.

10 The term shall not include:

11 1) services primarily designed for private interpersonal communication without
12 public or algorithmically recommended social-content features:

13 2) online learning management systems operated for legitimate educational
14 purposes;

15 3) government websites and services;

16 4) health, counseling, emergency, child-protection, or public-service platforms;

17 5) services primarily providing employment, professional, financial, or business
18 functions, unless they also operate social-media features; and

19 6) such other services as may be excluded by implementing rules based on their
20 primary purpose, functionality, and risk profile.

21 (d) "Child user" means a user whom a covered platform knows, reasonably believes,
22 or should reasonably have determined to be below eighteen (18) years of age.

23 (e) "Parental or guardian consent" means verifiable authorization given by a parent or
24 lawful guardian for the processing of a child's personal information and, where
25 applicable, the child's use of a covered platform.

(f) "High-risk processing" refers to processing of personal or sensitive personal information or platform activity presenting a significant risk to the rights, safety, dignity, or welfare of a child.

(g) "Age-restricted account" means an account subject to special safeguards because its user is below eighteen (18) years of age.

(h) "Recommender system" means an automated or algorithmic system that determines, prioritizes, recommends, ranks, or otherwise materially influences the content, accounts, advertisements, or interactions presented to a user.

(i) "Targeted advertising" means advertising directed to a user based on profiling, behavioral tracking, inferred characteristics, or other individualized processing of personal data.

SEC. 5. *Prohibition on Independent Social Media Accounts of Children Below Thirteen.*

– A child below thirteen (13) years of age shall not create, maintain, or independently operate a social-media account on a covered platform.

A covered platform shall, upon determining that an account is being operated by a child below thirteen (13) years of age, take reasonable measures to disable or restrict the account, subject to the notice, verification, and appeal procedures established under this Act.

Nothing in this Section shall prohibit a child below thirteen (13) from accessing:

(a) educational or learning services;

(b) government services;

(c) health, counseling, emergency, and child-protection services;

(d) age-appropriate communication services operated for legitimate family or educational purposes; or

(e) other services expressly exempted by the implementing rules.

1 **SEC. 6. *Social Media Access by Children Thirteen to Fifteen Years of Age.*** — A child
2 who is at least thirteen (13) but below sixteen (16) years of age may use a covered platform only
3 through an age-restricted account and subject to:

- 4 (a) verified parental or lawful guardian authorization;
- 5 (b) enhanced privacy and safety settings by default;
- 6 (c) restrictions on targeted advertising;
- 7 (d) restrictions on direct communications with adults who are not reasonably connected
8 to the child through an appropriate social or institutional relationship;
- 9 (e) access to parental supervision tools;
- 10 (f) age-appropriate content and recommendation controls;
- 11 (g) reasonable screen-time and break-management tools; and
- 12 (h) such additional safeguards as may be prescribed by the implementing agencies.

13 A parent or guardian may withdraw authorization at any time, subject to reasonable
14 procedures established by the platform.

15 **SEC. 7. *Social Media Access by Children Sixteen to Seventeen Years of Age.*** — A child
16 who is at least sixteen (16) but below eighteen (18) years of age may maintain an account on a
17 covered platform without mandatory parental consent.

18 Covered platforms shall nevertheless provide such users with:

- 19 (a) enhanced privacy settings by default;
- 20 (b) child-safety protections;
- 21 (c) restrictions on targeted advertising based on profiling or behavioral tracking;
- 22 (d) meaningful control over recommender systems;
- 23 (e) easy-to-use reporting and blocking mechanisms;
- 24 (f) protection against unsolicited adult contact and grooming;

- (g) screen-time and notification controls;
- (h) tools allowing the user to restrict discovery of the user's account;
- (i) clear and child-appropriate privacy notices; and
- (j) the right to obtain meaningful explanations concerning significant automated decisions affecting the user's access, safety, or account.

Nothing in this Section shall prevent a parent or guardian from providing voluntary supervision consistent with the child's age, maturity, best interests, and right to privacy.

SEC. 8. *Privacy-Preserving Age Assurance.* — Covered platforms shall establish reasonable and proportionate age-assurance mechanisms appropriate to the risks associated with their services.

Age assurance shall:

- (a) collect and process only the minimum information reasonably necessary;
- (b) avoid unnecessary retention of identity documents;
- (c) not require biometric information when a less intrusive method can reasonably accomplish the same purpose;
- (d) prohibit the use of age-assurance information for advertising, profiling, or unrelated commercial purposes;
- (e) implement appropriate technical and organizational security measures;
- (f) provide clear notice explaining the age-assurance process in child-appropriate language;
- (g) provide reasonable means to correct erroneous age determinations; and
- (h) comply with the principles of transparency, legitimate purpose, proportionality, data minimization, security, and accountability under the Data Privacy Act of 2012.

1 The National Privacy Commission shall issue standards governing privacy-preserving age
2 assurance.

3 SEC. 9. *Prohibition on Mandatory Government Identification as the Sole Method of Age*
4 *Verification.* – No covered platform shall be required to obtain or retain a government-issued
5 identification document from every user as the sole or mandatory method of age assurance.

6 The implementing rules shall establish a range of privacy-preserving methods appropriate
7 to the risk and functionality of the covered service.

8 SEC. 10. *Third-Party Age-Assurance Providers.* — A covered platform may engage an
9 independent third-party age-assurance provider.

10 Such provider shall:

11 (a) use age information solely for age-assurance purposes;

12 (b) maintain appropriate information-security safeguards;

13 (c) not sell, advertise, profile, or otherwise commercially exploit age-assurance
14 information;

15 (d) retain information only for the minimum period necessary;

16 (e) maintain auditable records of compliance; and

17 (f) comply with the Data Privacy Act of 2012 and regulations of the National Privacy
18 Commission.

19 The platform shall remain responsible for compliance notwithstanding its engagement of a
20 third-party provider.

21
22 SEC. 11. *Highest Reasonable Privacy and Safety Settings by Default.* — Covered
23 platforms shall provide child users with the highest reasonable privacy and safety settings
24 appropriate to their age.

25 Such settings shall include, where technically appropriate:

- (a) private-by-default profiles;
- (b) restricted discoverability;
- (c) restricted location sharing;
- (d) limits on unsolicited messages;
- (e) limits on direct contact from unknown adults;
- (f) restrictions on public sharing of sensitive information;
- (g) simplified blocking and reporting tools;
- (h) restrictions on the automatic addition of contacts;
- (i) enhanced account-security measures; and
- (j) mechanisms for rapid reporting of suspected abuse, exploitation, grooming, or other serious threats.

SEC. 12. *Prohibited Practices Directed at Child Users.* — A covered platform shall not:

- (a) knowingly design or deploy a feature primarily intended to induce excessive or compulsive use by children;
- (b) use deceptive or manipulative interface designs to prevent children or their parents from exercising privacy or safety choices;
- (c) knowingly encourage children to disable safety settings;
- (d) use sensitive personal data of children for targeted advertising;
- (e) sell or otherwise commercially exploit children's personal data;
- (f) intentionally expose child users to advertisements for prohibited or age-inappropriate products or services;
- (g) intentionally facilitate contact between children and persons reasonably suspected of grooming, exploiting, or abusing children; or
- (h) use a child's personal information to infer highly sensitive characteristics for advertising or behavioral manipulation.

SEC. 13. *Child-Safe Recommender Systems.* — Covered platforms whose services use recommender systems shall implement reasonable measures to prevent the algorithmic recommendation or amplification of content reasonably likely to cause serious harm to child users.

1 Platforms shall conduct periodic risk assessments concerning:

- 2 (a) content recommendation;
- 3 (b) engagement-maximization systems;
- 4 (c) advertising;
- 5 (d) direct messaging;
- 6 (e) account discoverability; and
- 7 (f) other automated systems materially affecting children.

8 SEC. 14. *Limits on Behavioral Profiling of Children.* — A covered platform shall not
9 engage in behavioral profiling of a child for targeted advertising.

10 The processing of children's personal information for advertising shall be limited to
11 contextual or otherwise non-profiling advertising that does not exploit the child's personal
12 information or behavioral history.

13 SEC. 15. *Transparency of Automated Systems.* — Covered platforms shall publish child-
14 accessible explanations of the principal factors affecting:

- 15 (a) content recommendations;
- 16 (b) account recommendations;
- 17 (c) advertisements;
- 18 (d) visibility or discoverability; and
- 19 (e) enforcement decisions affecting child users.

20 Nothing in this Section shall require disclosure of trade secrets, source code, security-
21 sensitive information, or proprietary information beyond what is reasonably necessary to ensure
22 meaningful transparency.

23 SEC. 16. *Parental and Guardian Tools.* — For users below sixteen (16) years of age,
24 covered platforms shall make available, at no additional cost:

- 25 (a) account privacy controls;
- 26 (b) screen-time and break-management tools;

- (c) controls for direct messaging;
- (d) controls over discoverability;
- (e) mechanisms for reporting harmful content;
- (f) notification and activity controls; and
- (g) mechanisms for withdrawing consent where parental consent is required.

Parental tools shall not automatically provide access to the content of private communications except where specifically authorized by the child, required by law, or necessary to address a credible and serious threat to the child's safety.

SEC. 17. ***Rights of Child Users.*** — A child user shall have the right to:

- (a) age-appropriate privacy;
- (b) clear and understandable information regarding the processing of personal data;
- (c) request correction of inaccurate personal information;
- (d) report abuse, exploitation, bullying, harassment, and harmful content;
- (e) block or restrict other users;
- (f) appeal an automated account restriction or suspension;
- (g) obtain an explanation of a material enforcement decision affecting the account;
- (h) access age-appropriate educational resources concerning digital safety; and
- (i) be heard in decisions materially affecting the child's digital participation, consistent with the child's age and maturity.

SEC. 18. ***Duty and Care.*** — Covered platforms shall exercise reasonable care proportionate to the foreseeable risks of their services to child users.

The duty under this Section shall include reasonable measures concerning:

- (a) age assurance;
- (b) privacy;
- (c) content safety;
- (d) recommender systems;
- (e) advertising;

- (f) account security;
- (g) grooming and exploitation;
- (h) cyberbullying;
- (i) reporting and complaints; and
- (j) platform design.

SEC. 19. ***Child Online Safety Impact Assessment.*** — A covered platform with a significant number of users in the Philippines shall conduct a Child Online Safety Impact Assessment before introducing a new feature reasonably likely to create significant risks to children.

The assessment shall identify:

- (a) foreseeable risks;
- (b) categories of affected children;
- (c) privacy risks;
- (d) risks arising from algorithmic recommendations;
- (e) measures to mitigate identified risks; and
- (f) mechanisms for monitoring and correcting unforeseen harms.

The National Privacy Commission and the Department of Information and Communications Technology shall jointly issue standards for such assessments.

SEC. 20. ***Reporting of Serious Child-Safety Incidents.*** — Covered platforms shall maintain mechanisms for reporting serious child-safety incidents.

Where required by existing law, platforms shall promptly report suspected online sexual abuse or exploitation of children and other criminal activity to the appropriate government authorities.

Nothing in this Act shall diminish any mandatory reporting obligation under existing law.

SEC. 21. ***Transparency Reports.*** — Covered platforms shall submit an annual Child Online Safety Transparency Report to the Department of Information and Communications Technology containing, in aggregate and anonymized form:

- (a) the number of child accounts subject to age restrictions;
- (b) age-assurance failures and corrections;
- (c) accounts disabled for violation of child-access requirements;
- (d) reports involving child exploitation, grooming, bullying, and serious threats;
- (e) response and resolution times;
- (f) enforcement actions;
- (g) complaints and appeals;
- (h) significant changes to recommender systems affecting children; and
- (i) other information required by the implementing rules.

No report shall contain personally identifiable information of individual children.

SEC. 22. *Inter-Agency Child Digital Safety Council.* — There is hereby created a Child Digital Safety Council, composed of:

- (a) the Department of Information and Communications Technology (DICT), as Chair;
- (b) the National Privacy Commission;
- (c) the Department of Social Welfare and Development;
- (d) the Department of Education;
- (e) the Department of Justice;
- (f) the National Telecommunications Commission;
- (g) the Philippine National Police Anti-Cybercrime Group;
- (h) the Department of Health; and
- (i) such other government agencies as may be designated by the President.

The Council shall coordinate policy, enforcement, education, research, and implementation of this Act.

SEC. 23. *Powers and Functions.* — The Council shall:

- (a) develop national standards for child digital safety;
- (b) coordinate enforcement among government agencies;
- (c) develop public education programs;

- (d) establish procedures for inter-agency complaints;
- (e) commission studies on children's digital welfare;
- (f) monitor emerging technologies and platform practices;
- (g) recommend legislative and regulatory amendments; and
- (h) submit an annual report to Congress on the implementation of this Act.

SEC. 24. *Role of the National Privacy Commission.* — The National Privacy Commission shall have primary authority over matters involving the processing, collection, retention, disclosure, security, and protection of children's personal data under this Act.

The Commission shall issue regulations concerning:

- (a) age assurance;
- (b) children's privacy;
- (c) data minimization;
- (d) retention and deletion;
- (e) biometric information;
- (f) profiling;
- (g) targeted advertising; and
- (h) privacy impact assessments.

SEC. 25. *Role of the Department of Information and Communications Technology.* — The DICT shall establish technical and operational standards concerning:

- (a) platform compliance;
- (b) age-assurance interoperability, where appropriate;
- (c) cybersecurity;
- (d) reporting mechanisms;
- (e) transparency;
- (f) technical audits; and
- (g) child-safety-by-design standards.

SEC. 26. *Administrative Violations.* — A covered platform may be held administratively liable for:

- (a) knowingly permitting prohibited accounts below the minimum age after reasonable notice and opportunity to correct;
- (b) failure to implement required age-assurance mechanisms;
- (c) failure to implement mandated child-safety measures;
- (d) unlawful processing or commercial exploitation of children's personal data;
- (e) prohibited behavioral profiling;
- (f) failure to comply with reporting obligations;
- (g) submission of materially false compliance reports;
- (h) repeated failure to respond to serious child-safety complaints; or
- (i) other violations established by the implementing rules.

SEC. 27. *Administrative Fines.* — After notice and hearing, the appropriate regulatory authority may impose the following administrative fines:

- (a) First violation: not less than Five Million Pesos (₱5,000,000) but not more than Ten Million Pesos (₱10,000,000);
- (b) Second violation: not less than Ten Million Pesos (₱10,000,000) but not more than Twenty-Five Million Pesos (₱25,000,000); and
- (c) Subsequent or grave violations: not less than Twenty-Five Million Pesos (₱25,000,000) but not more than Fifty Million Pesos (₱50,000,000).

In determining the amount of the fine, the authority shall consider:

- 1) the nature, gravity, and duration of the violation;
- 2) the number and vulnerability of affected children;
- 3) whether the violation was intentional, reckless, or negligent;
- 4) the platform's size and capacity;
- 5) previous violations;
- 6) cooperation with authorities;

- 7) remedial measures; and
- 8) the economic benefit obtained from the violation.

SEC. 28. *Continuing Violations.* — Where a violation continues after receipt of a final order directing corrective action, an additional administrative fine of not more than One Hundred Thousand Pesos (₱100,000) per day may be imposed until compliance, subject to the limitations and procedures prescribed by the implementing rules.

SEC. 29. *Corrective Orders.* — In addition to fines, the appropriate authority may issue:

- (a) compliance orders;
- (b) corrective-action orders;
- (c) orders requiring deletion or cessation of unlawful processing;
- (d) orders requiring modification of unlawful platform practices;
- (e) temporary suspension of a particular feature presenting an imminent and substantial risk to children; or
- (f) other proportionate remedies authorized by law.

SEC. 30. *Temporary Restriction of Platform Operations.* — Where a covered platform repeatedly commits grave violations and fails to comply with final corrective orders, the appropriate authority may recommend to the proper government authority the temporary restriction of specified platform functions or access in the Philippines.

Any restriction under this Section shall:

- (a) be based on substantial evidence;
- (b) be proportionate to the violation;
- (c) be limited to the extent reasonably necessary;
- (d) observe due process;
- (e) provide an opportunity for judicial review; and
- (f) consider the effect on lawful users and access to essential services.

A complete prohibition of a platform shall be an extraordinary remedy available only for repeated, grave, and continuing violations where lesser measures have demonstrably failed.

1 SEC. 31. ***No Criminal or Administrative Penalty Against Children.*** — A child shall not
2 be criminally or administratively punished solely for:

- 3 (a) creating an account in violation of the age restrictions under this Act;
- 4 (b) providing an incorrect age to a platform; or
- 5 (c) accessing a covered platform contrary to the platform's age restrictions.

6 The primary responsibility for compliance shall rest upon covered platforms and, where
7 applicable, adults who knowingly assist in circumventing the protections established by this Act.

8 Nothing in this Section shall exempt a child from liability under other laws for independent
9 criminal conduct unrelated to the mere violation of an age restriction.

10 SEC. 32. ***National Digital Safety Education Program.*** — The Department of Education,
11 in coordination with DICT, DSWD, NPC, DOH, and other relevant agencies, shall establish a
12 continuing national program on:

- 13 (a) digital literacy;
- 14 (b) privacy and cybersecurity;
- 15 (c) cyberbullying prevention;
- 16 (d) online sexual exploitation prevention;
- 17 (e) media and information literacy;
- 18 (f) responsible social-media use;
- 19 (g) healthy technology habits;
- 20 (h) misinformation and disinformation awareness;
- 21 (i) recognizing grooming and online manipulation; and
- 22 (j) reporting and seeking assistance for online harms.

23 SEC. 33. ***Parent and Guardian Education.*** — The government shall provide parents and
24 guardians with accessible materials concerning:

- 25 (a) age-appropriate technology use;
- 26 (b) parental controls;
- 27 (c) online privacy;

- 1 (d) recognizing online exploitation;
- 2 (e) cyberbullying;
- 3 (f) mental and emotional well-being in the digital environment; and
- 4 (g) responsible and non-invasive digital supervision.

5 SEC. 34. *Notice and Appeal.* — A child or parent/guardian affected by an account
6 restriction shall be provided a reasonably accessible mechanism to challenge the decision.

7 A covered platform shall maintain a process for correcting erroneous age determinations
8 and restoring accounts wrongfully restricted.

9 SEC. 35. *Protection Against Overblocking.* — Nothing in this Act shall require a covered
10 platform to remove lawful content merely because it may be unsuitable for some children.

11 Platforms shall adopt proportionate measures, including age-rating, content controls,
12 restricted recommendations, and user controls, where complete removal is not required by law.

13 SEC. 36. *Protection of Constitutional Rights.* — The implementation of this Act shall
14 respect:

- 15 (a) freedom of speech and expression;
- 16 (b) freedom of the press;
- 17 (c) freedom of association;
- 18 (d) right to privacy;
- 19 (e) right to due process;
- 20 (f) right to access information; and
- 21 (g) the best interests and evolving capacities of the child.

22 No provision of this Act shall be interpreted to authorize generalized government
23 surveillance of children or the population.

24 SEC. 37. *Registration and Compliance Declaration.* — Covered platforms operating in
25 the Philippines shall comply with registration, designation, reporting, and other reasonable
26 regulatory requirements prescribed by the DICT, consistent with existing law.

1 No registration requirement shall be used as a means of imposing prior restraint on lawful
2 expression.

3 SEC. 38. ***Phased Implementation.*** — The requirements of this Act shall be implemented
4 in phases:

5 (a) Within six (6) months from effectivity, the implementing agencies shall promulgate
6 the implementing rules and regulations;

7 (b) Within twelve (12) months from effectivity, covered platforms shall implement the
8 basic child-safety, privacy, reporting, and parental-control requirements;

9 (c) Within eighteen (18) months from effectivity, covered platforms shall implement
10 the required age-assurance mechanisms;

11 (d) Within twenty-four (24) months from effectivity, all covered platforms shall
12 comply fully with the recommender-system, transparency, and child-safety impact-
13 assessment requirements.

14 The implementing agencies may provide reasonable extensions where a platform
15 demonstrates substantial technical necessity and continued protection of children.

16 SEC. 39. ***Regulatory Sandbox.*** — The DICT and National Privacy Commission may
17 establish a regulatory sandbox allowing qualified technology providers and covered platforms to
18 test privacy-preserving age-assurance and child-safety technologies under controlled conditions.

19 No technology tested under the sandbox shall be deployed nationally unless it complies
20 with applicable privacy, cybersecurity, and child-protection requirements.

21 SEC. 40. ***Appropriations.*** — The amount necessary for the initial implementation of this
22 Act shall be charged against the current appropriations of the DICT, DSWD, DepEd, NPC, and
23 other concerned agencies.

24 Thereafter, such sums as may be necessary for the continued implementation of this Act
25 shall be included in the annual General Appropriations Act.

1 SEC. 41. ***Implementing Rules and Regulations.*** — Within six (6) months from the
2 effectivity of this Act, the DICT, NPC, DSWD, DepEd, DOJ, NTC, DOH, and other concerned
3 agencies shall jointly promulgate the implementing rules and regulations.

4 The IRR shall be developed with consultation from:

- 5 (a) children and youth representatives;
- 6 (b) parents and guardians;
- 7 (c) educators;
- 8 (d) child-protection organizations;
- 9 (e) privacy and cybersecurity experts;
- 10 (f) technology companies;
- 11 (g) telecommunications and internet-service providers;
- 12 (h) mental-health professionals;
- 13 (i) human-rights organizations; and
- 14 (j) other relevant stakeholders.

15 SEC. 42. ***Congressional Oversight.*** — The appropriate committees of the Senate and
16 House of Representatives shall conduct a mandatory review of the implementation of this Act not
17 later than three (3) years after its effectivity and every three (3) years thereafter.

18 The review shall consider:

- 19 (a) effectiveness of age restrictions;
- 20 (b) privacy impacts;
- 21 (c) effectiveness of age-assurance technologies;
- 22 (d) rates of cyberbullying and online exploitation;
- 23 (e) impact on children's mental and social well-being;
- 24 (f) effects on education and access to information;
- 25 (g) platform compliance;
- 26 (h) enforcement outcomes; and
- 27 (i) developments in technology.

1 SEC. 43. *Separability Clause.* — If any provision of this Act is declared unconstitutional
2 or invalid, the remaining provisions not affected thereby shall continue to be in full force and
3 effect.

4 SEC. 44. *Repealing Clause.* — All laws, decrees, orders, rules, regulations, and other
5 issuances or parts thereof inconsistent with the provisions of this Act are hereby repealed,
6 amended, or modified accordingly.

7 SEC. 45. *Effectivity.* — This Act shall take effect fifteen (15) days after its complete
8 publication in the Official Gazette or in a newspaper of general circulation.

9 Approved,