Global Platform *for* Child Exploitation Policy

Thailand

Legal questionnaire completed by Tilleke & Gibbins International Ltd. • June 2024

This document contains responses from the law firm listed above to a questionnaire distributed by NCMEC (questions are in **bold text**). Responses to the questionnaire may be limited to officially enacted legislation; it is possible that actual practice or enforcement of the law varies, and relevant court rulings or case law may also differ from legislative text. Responses have been reformatted and may have been slightly edited for clarity. Furthermore, responses may include commentary, paraphrasing, and unofficial translations of source material (e.g., national legislation) originally produced in other languages. Only official source documents in official languages should be relied upon as legally binding. This document serves to inform further research and does not constitute legal advice from NCMEC or the listed law firm.

1. **What laws and regulations contain legal definitions of the following terms or corresponding terms in your local jurisdiction (links to existing U.S. legal definitions are included, where relevant, as background for comparison – please include definitions of any corresponding terms in your country):**

    a. **child or minor (18 U.S.C. 2256(1), https://www.law.cornell.edu/uscode/text/18/2256)**

        i. Child Protection Act B.E. 2546 (2003): Under Section 4, "child" means a person whose age is less than 18 years but does not include those who attain majority through marriage.

        https://www.moe.go.th/backend/wp-content/uploads/2021/02/809775_0001.pdf

        ii. National Child and Youth Development Promotion Act B.E. 2550 (2007): Under Section 4, "child" means a person below 18 years of age. "Youth" means a person between 18 to 25 years of age.

        https://law.m-society.go.th/law2016/uploads/lawfile/593509b4e06d5.pdf

        iii. Civil and Commercial Code ("CCC"): The definition of child or minor is not specifically provided under the CCC, but Section 19 states that on completion of 20 years of age, a person ceases to be a minor and becomes sui juris.

        https://www.ocs.go.th/council-of-state/#/public?%2F=

        iv. Anti-Trafficking in Persons Act B.E. 2551 (2008): Under Section 4, "child" means any person under 18 years of age.

        https://oia.coj.go.th/th/file/get/file/20190212cfc8f33d0e0edd2310abb030b61bb882160403.PDF

        We note that our research and responses to this question and the others in this questionnaire have taken into account international treaties which have been incorporated into domestic law.

    b. **child sexual exploitation (Missing Children's Assistance Act of 2023, Section 2, (a)(1)(9), https://www.congress.gov/118/bills/s2051/BILLS-118s2051es.pdf)**

i. Criminal Code – There is no definition of "child sexual exploitation" under the Criminal Code. However, there is an offence related to child sexual exploitation related to child pornography. Section 287/1 and Section 287/2 of the Criminal Code stipulate that the trading, distribution, exhibition, production, possession, import, export of child pornography is subject to imprisonment not exceeding 10 years and/or a fine not exceeding THB 200,000.

https://www.ocs.go.th/council-of-state/#/public?%2F=

ii. Anti-Trafficking in Person Act B.E. 2551 (2008) – Section 6 provides the definition of exploitation as seeking benefits from prostitution, production or distribution of pornographic materials, other forms of sexual exploitation, slavery, causing another person to be a beggar, forced labour or service, coerced removal of organs for the purpose of trade, or any other similar practices resulting in forced extortion, regardless of such person's consent.

https://oia.coj.go.th/th/file/get/file/20190212cfc8f33d0e0edd2310abb030b61bb882160403.PDF

c. **sexually explicit conduct (18 U.S.C. 2256(2), https://www.law.cornell.edu/uscode/text/18/2256)**

There is no definition of "sexually explicit conduct" under Thai law. However, Section 4 of the Criminal Code provides the definition of sexual assault as any action for the satisfaction of the offender by using the offender's genitals to invade another person's genitals, anus, or mouth.

https://www.ocs.go.th/council-of-state/#/public?%2F=

d. **child sexual abuse (18 U.S.C. 2243(a), https://www.law.cornell.edu/uscode/text/18/2243)**

There is no definition of "child sexual abuse" or "abuse" under Thai law. Any determination by a court of whether an action would be deemed as "child sexual abuse" or "abuse" would be on a case-by-case basis. For example, any action with the intention to take advantage of a child would be considered as child abuse. For sexual abuse, it would be any forced action involving physical intrusion of the other person.

e. **child pornography or child sexual abuse material (CSAM) (18 U.S.C. 2256(8), https://www.law.cornell.edu/uscode/text/18/2256)**

i. Criminal Code – Section 1 (17). Note that the definition of "child pornography" has been added by the Act Amending the Criminal Code (No. 24) B.E. 2558 (2015). (We note, however that an official English translation of this is not available.)

ii. "Child pornography" under the Criminal Code means an object or thing which is understood as or depicts the sexual acts of a child or with a child who is not over eighteen years of age through images, stories or in a manner that can be understood as pornographic, whether in the form of a document, drawing, print, painting, printed

matter, picture, advertised image, symbol, photograph, movie, audio tape, video tape or any other similar form, and shall include the object or thing above which is stored in computer systems or other electronic equipment that can show understandable results.

https://www.ocs.go.th/council-of-state/#/public?%2F=

f. computer-generated images or videos of child pornography or CSAM (created by artificial intelligence or morphed) (18 U.S.C. 2256(8) & (9), https://www.law.cornell.edu/uscode/text/18/2256)

There are no separate definitions of computer-generated images or videos of child pornography or CSAM, but these would be covered under the definition of "child pornography" under the Criminal Code.

g. enticement or grooming (encouraging, persuading, or coercing a child to engage in sexual activity or to create child pornography or CSAM) (18 U.S.C. 2422(b), https://www.law.cornell.edu/uscode/text/18/2422)

i. There is no definition of "enticement" or "grooming" under Thai law, but Section 282, § 283, Section 283 bis and Section 284 of the Criminal Code stipulate offences related to procuring, luring, or trafficking of a person aged 15 – 18 for an indecent sexual purpose regardless of the victims' consent.

ii. Procuring, luring, persuading of a person for prostitution regardless of such person's consent is also considered an offence under Section 9 of the Prevention and Suppression of Prostitution Act B.E. 2539 (1996).

https://www.refworld.org/legal/legislation/natlegbod/1996/en/58177

h. legal age of consent for sexual activity – are there laws and regulations, if so, what ages are specified?

There is no provision under Thai law specifically providing a legal age of consent for sexual activity. Having said that, Section 19 of the Civil Code sets the general legal age of consent for legal acts at the age of 20 years old. Also of relevance here, Section 277 of the Criminal Code states that regardless of the victim's consent, sexual assault of a person under the age of 15 who is not the offender's spouse is considered a crime.

https://www.ocs.go.th/council-of-state/#/public?%2F=

i. Sextortion (extorting money or sexual favors from a child by threatening to share sexually explicit, child pornography or CSAM images of the child) (Missing Children's Assistance Act of 2023, Section 2, (a)(1)(8), https://www.congress.gov/118/bills/s2051/BILLS-118s2051es.pdf)

There is no definition of sextortion under Thai law. The Criminal Code does not include an offence specifically for sextortion, but only stipulates extortion under Section 337 as an act or a threat to act of violence against the life, body, liberty, reputation or property of the victim or a third person so that the victim submits to the same is said to commit extortion and

blackmailing under Section 338 as threatening to disclose the secret, to cause injury to the victim or the third person, up to the victim submit to the same.

https://www.ocs.go.th/council-of-state/#/public?%2F=

2. **Please explain any legal or regulatory requirement or recommendation for Online Platforms to undertake any of the following activities on their systems to protect children online from sexual exploitation:**

   a. **review, screen, moderate, or detect content to identify child pornography or CSAM content**
   b. **review, screen, moderate, or detect content to identify enticement, grooming, or sextortion of a child**
   c. **report child pornography, CSAM, enticement, grooming, or sextortion that they become aware of or are notified about on their systems to a law enforcement or government agency or nongovernmental organization**
   d. **remove or take down any child pornography, CSAM, enticement, grooming, or sextortion that they identify, become aware of, or are notified about**
   e. **review content by human moderators to screen or moderate for child pornography or CSAM**
   f. **remove child pornography, CSAM, enticement, grooming, or sextortion from their systems when notified of its presence by a victim, nongovernmental organization, law enforcement, or government agency**
   g. **use any specific technology to detect, remove, block, or take down any child pornography, CSAM, enticement, grooming, or sextortion, including:**
      i. **"Hashing technology" (https://www.thorn.org/blog/hashing-detect-child-sex-abuse-imagery/). Many Online Platforms hash and tag images and videos of child pornography or CSAM and then use hashing technology to scan content on their systems to detect the distribution of child pornography or CSAM online so it can be removed.**
      ii. **Artificial intelligence or machine learning tools to detect the presence of child pornography, CSAM, enticement, grooming, or sextortion.**
   h. **if the applicable laws or regulations require some, but not all, Online Platforms to perform any of the above activities, describe how the differing requirements apply. For example, are differences based on the number of online users, types of services offered, etc.?**

There are no legal requirements for Online Platforms with respect to the above-mentioned activities to protect children from sexual exploitation online. Having said that, there are some activities to protect children, i.e., removing child pornography, CSAM, enticement, grooming, or sextortion from the systems, but these must be ordered by a court as remedies in a case where an injured party files a lawsuit with the court against a defendant under the Computer-Related Crime Act B.E. 2550 (2007). The relevant sections under this Act under which a person would file a lawsuit are Sections 14, 16/1 and 16/2.

Under Section 14 of the Computer-Related Crime Act B.E. 2550 (2007), any person who perpetrates the offence of putting into a computer system any computer data which is obscene and that may be accessible by the public, the perpetrator or a person who distributes or transfers the computer data shall be subject to imprisonment not exceeding three years and a fine not exceeding sixty thousand baht, or both. We also note that this is a compoundable offence, which means that the victim can

agree to withdraw the complaint from the court and the offender will not be subject to criminal liabilities.

After the court renders the judgment and the defendant is found guilty in accordance with section 14, the court may give an order to destroy/ remove the data of child pornography, CSAM, enticement, grooming, or sextortion. This is in accordance with sections 16/1 and 16/2 of the Computer-Related Crime Act B.E. 2550 (2007) as amended by the Computer-Related Crime Act (No. 2) B.E. 2560 (2017) ("CCA").

Further to removing or taking down the data, Section 16/1 of the CCA specifies that the court may give an order to publish or disseminate in whole or in part the verdict that the defendant was found guilty in electronic media, broadcast radio, television or newspapers, as deemed fit by the court, at the expense of the accused; and/or to perform other measures as deemed fit by the court in order to mitigate the damages from the offence.

3. **Are Online Platforms legally required or recommended to implement any method to verify the age of a user before allowing access to an online platform?**

There is no legal requirement for Online Platforms to implement any method to verify the age of the user before accessing the online platform. Further, we found no official recommendations with respect to the implementation of such methods.

However, nearly every online platform in Thailand has its own requirement of a minimum age to open an account. Examples of the required minimum ages are as follows:

- Facebook: 13 years old
- Instagram: 13 years old
- Twitter: 13 years old
- TikTok: 13 years old
- Line: 12 years old
- YouTube: 18 years old; however, a 13-year-old child can register if the child obtains consent from his/ her parent or guardian.

Despite these requirements of the platform, which are displayed on each site's "Terms of Use" page, it is not uncommon for children to enter fake age information in order to open an account.

We also note that the Royal Thai Police have established the Thailand Internet Crimes Against Children Taskforce ("TICAC"). TICAC provides some information on its website to raise awareness of online child abuse, but it does not provide any specific recommendations with respect to age verification, parental consent, etc.

4. **Are Online Platforms legally required or recommended to implement any method to obtain parental consent before a child uses the services of such Online Platforms?**

Thailand does not have any law specifically requiring Online Platforms to obtain parental consent before a child uses their services.

However, as discussed in more detail below, Thailand does have personal data protection legislation which is aimed at the protection of the personal data of all individuals, not just children. Broadly speaking (and recognizing that there are various exceptions to the general rules), under this

legislation, an Online Platform is required to obtain the consent of any individual before collecting, using, or disclosing their personal data. Where the individual is a minor, the legislation would require the Online Platform to obtain the consent of the parent or guardian. Again, although Thailand does not have legislation that specifically requires Online Platforms to obtain parental consent before a child uses their services, in practice, and as discussed further below, the consent requirements of the personal data protection legislation could potentially require them to do so.

The relevant law here is Thailand's Personal Data Protection Act, B.E. 2562 (2019) ("PDPA") which provides that a "Data Controller" (as defined under the PDPA) shall not collect, use, or disclose "Personal Data" (as defined under the PDPA), unless the data subject has given consent prior to or at the time of such collection, use, or disclosure, except where it is permitted to do so by other provisions of the PDPA or any other laws.

Under Section 20 of the PDPA, parental consent is required for a minor under the age of 10 to provide his or her Personal Data to a Data Controller (i.e., the Online Platform). However, with respect to the Personal Data of a minor over the age of 10 (which, subject to certain exceptions, would be an individual under the age of 20), the situation would be up to the determination of a Thai court.

For minors over the age of 10, Section 20 of the PDPA provides that the Data Controller must also obtain the consent of the parent or guardian of the minor, unless providing Personal Data to the Data Controller would be considered by a Thai court to be an act of a nature for which the CCC recognizes that the minor may be entitled to act alone (i.e., without parental consent). As set out below in Sections 22-24 of the CCC, these acts would ones in which the minor "merely acquires a right or is freed from a duty"; or an act which is "strictly personal"; or an act which would be considered "suitable to [the minor's] condition in life, and actually required for his or her reasonable needs."

The question, then, would be whether a Thai court would consider providing Personal Data the type of act which would fall under Section 22-24 and for which a minor over the age of 10 would not need parental consent.

While we did not find any Supreme Court precedent cases addressing this issue, it is our assessment that it is likely that a minor over the age of 10 and/or an Online Platform would have a valid argument that simply providing the Personal Data necessary to sign up for an online platform would fall under one of the provisions of Sections 22-24 of the CCC (particularly the "strictly personal" exception under Section 23). We base this assessment on other precedent cases in which a Thai court has examined whether a minor would be able to enter into an act without parental consent. Assuming that signing up for the Online Platform does not require the minor to enter into any monetary contract and/or any other transaction of significant monetary value, and assuming that the minor is simply providing some basic information to open an account (i.e., name, date of birth, email address, etc.), we believe that it is likely that a Thai court would find that such act would fall under one of the provisions of Sections 22-24.

https://www.mdes.go.th/uploads/tinymce/source/%E0%B8%AA%E0%B8%84%E0%B8%AA/Personal%20Data%20Protection%20Act%202019.pdf

Please also refer to Sections 22, 23, and 24 of the CCC (as referenced in Section 20 of the PDPA):

Section 22
A minor can do all acts by which he or she merely acquires a right or is freed from a duty.

Section 23
A minor can do all acts which are strictly personal.

Section 24
A minor can do all acts which are suitable to his or her condition in life, and actually required for his or her reasonable needs.

https://www.ocs.go.th/council-of-state/#/public?%2F=

5. **Are there legal remedies for children who have been victimized by online child sexual exploitation? This may include children who are victimized by the distribution of child pornography or CSAM imagery in which they are depicted, or children victimized by enticement, grooming or sextortion. If such legal remedies exist, do they include:**

   YES

   a. **The ability to stop the publication of the pornography or CSAM imagery by the Online Platform?**
   b. **An obligation on the part of the Online Platform to take active steps to remove the pornography or other imagery from their servers?**
   c. **An ability to get an injunction or other court order against the Online Platform to stop them from publishing the pornography or imagery?**
   d. **A protective order or other court order that prohibits the person who posts the pornography or imagery from doing so in the future on the same or other Online Platform?**
   e. **the ability to seek financial damages or any sort of monetary recovery from an offender who has shared the child's image or video, either in a civil or a criminal proceeding?**
   f. **the ability to seek any other forms of victim compensation/recovery/services provided for under the law and/or by a government-funded source?**
   g. **notification to a victim when an offender is arrested for distributing child pornography or CSAM in which the child is depicted?**

      Yes. Children who have been victimized by online child sexual exploitation can seek legal remedies under both civil and criminal law. This means that a child victim can request both monetary compensation and also that criminal liabilities be imposed on the offender. The specific provisions under which a victim could potentially seek these remedies include the following:

      Civil and Commercial Code
      - Wrongful act (i.e., tort / negligence) - Section 420

      Criminal Code
      - Offences relating to sexuality - Sections 282, 283, 283 bis, 284, 287/1, 287/1, and 287/2
      - Extortion - Section 337

      Prevention and Suppression of Prostitution Act B.E. 2539 (1996)

- Section 9

Computer-related Crime Act

- Sections 14, 16/1, and 16/2

For civil cases, the remedies depend on the request of the victim. It is possible for the victim to request that the court grant any of the remedies mentioned in a – g above. However, the court will consider granting the remedy as requested based on the evidence presented in the case and it might also be subject to specific requirements under procedural laws.

For example, the victim can request that the court issue an injunction order on the condition that the main complaint shall be filed to the court. The request for an injunction order must be related to the remedies sought in the main complaint. The victim can also ask the court to issue and emergency injunction order if the victim can prove that if the offence does not stop immediately, it will cause irreparable damage.

For criminal offences, the potential punishments under Thai law include the death penalty, imprisonment, confinement, fines and forfeiture of property. Sexual offences related to children are normally subject to fines and/or imprisonment. Additionally, police officers have the authority to confiscate the items used in committing crimes.

Moreover, Section 16/1 of the CCA provides additional remedies for victims. Section 14 of the CCA prohibits a person from putting any data into a computer system that is “obscene” and that may be accessible by the public. If a victim of such crime files a lawsuit and if the defendant is found guilty of Section 14, the defendant shall be subject to imprisonment, or a fine, or both.

What data is deemed “obscene” under the CCA should be considered with reference to the meaning of “child pornography” under the Criminal Code, Section 1 (17), as discussed above.

Under section 16/1 of the CCA, the court may give an order to destroy/ take down the data to prevent the distribution of child pornography or CSAM. Further, section 16/2 provides that whoever knows that the computer data which is in his/her possession is obscene computer data that is subject to being destroyed by the order of the court under section 16/1, must destroy such computer data; failing which, he/she shall be subject to imprisonment, or a fine, or both.

Another remedy is under section16/1 (2) of the CCA, which provides that the court may order the defendant/perpetrator to publish or disseminate in whole or in part the verdict that the perpetrator is found guilty and/or to apologize to the victim in electronic media, broadcast radio, television or newspapers, as deemed fit by the court, at the expense of the defendant/perpetrator.

Service providers have an obligation to comply with the CCA to destroy/ take down the obscene data from their system in accordance with Section 15; otherwise, the service providers shall be subject to the same penalty as the offender under Section 14.

Please see the full provisions of section s 14, 15, 16/1 and 16/2 of the CCA below.

Section 14

Whoever commits the following offences shall be liable to imprisonment for a term not exceeding five years, or a fine not exceeding One Hundred Thousand Baht, or both.

(1) Dishonestly or by deception, entering wholly or partially distorted or false computer data into a computer system in a manner likely to cause damage to the general public; which is not a defamation under the Criminal Code;
(2) Entering false computer data into a computer system in a manner which is likely to cause damage to the protection of national security, public safety, economic safety of the Kingdom of Thailand, infrastructures which are for public benefit; or to cause panic to the general public;
(3) Entering into a computer system, any computer data which is an offence related to national security of the Kingdom of Thailand or related to terrorism under the Criminal Code;
(4) Entering any obscene data into a computer system which could be accessed by the general public; or
(5) Disseminating or forwarding computer data despite knowing of the fact that it is computer data under (1), (2), (3), or (4) above.

In case the offence under paragraph (1) is not committed against the general public but rather against a certain person, the offender, the disseminator or the forwarder of such computer data shall be liable to an imprisonment for a term not exceeding three years, a fine not exceeding Sixty Thousand Baht or both; and such offence shall be deemed a compoundable offence.

Section 15

A service provider, who cooperates, consents or supports the perpetration of the offences under section 14 by using a computer system under his/her control, shall be liable to the same penalty as the offender under section 14.

The Minister shall issue a Notification specifying the process of warning, as well as blocking the dissemination of such computer data and removal of such computer data from the computer system.

A service provider who can prove that he/she has complied with the Notification of the Ministry issued under Paragraph 2, shall not be subject to the penalty.

Section 16/1*

As to the offense under section 14 or section 16, based on which the accused has been found guilty by the court, the court may give an order:

(1) to destroy the data under such Section;
(2) to publish or disseminate in whole or in part the verdict in electronic media, broadcast radio, television or newspapers, as deemed fit by the court, at the expense of the accused;
(3) to perform other measures as deemed fit by the court in order to mitigate the damages from the offense.

(*This section is amended by the Computer-related Crime Act (No. 2) B.E. 2560 (2017), Section 11.)

Section 16/2*

Any person who is aware that computer data in their possession is the data ordered for destruction as to section 16/1, the person is obliged to destroy such data. Any violation shall result in the person having to serve half of the penalty as provided for by the law in section 14 or section 16, as the case may be.

(*This section is amended by the Computer-related Crime Act (No. 2) B.E. 2560 (2017), Section 11.)

6. **"Safety by Design" is defined as tools or processes that are built into an Online Platform to protect children by making it easier for the relevant Online Platform to detect or prevent the distribution of child pornography or CSAM.**

   a. **Are Online Platforms legally required to incorporate "Safety by Design" into their systems?**

      No, Online Platforms are not legally required to incorporate "Safey by Design" into their systems at the time of establishment/initiation of those systems. However, as noted above, the CCA provides Thai courts with the authority to require defendants to implement appropriate measures to minimize potential damages incurred from wrongdoing.

      i. **If so, must these steps be taken before the launch of an Online Platform?**
      ii. **If so, if an Online Platform has already been in public use, when must they have incorporated "Safety be Design" measures?**
      iii. **For each of 6(a)(i) or (ii) above, please describe the legal requirement or recommendation.**

   b. **Please include information about the parameters for monitoring, management, and enforcement of any legal or regulatory requirements for the Online Platform's incorporation of "Safety by Design"?**

      As noted above, Online Platforms are not legally required to incorporate "Safety by Design" into their systems.