

Legal questionnaire completed by ABNR Counsellors at Law • April 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>)

The definition of 'child' has been set out in various laws in Indonesia, including but not limited to the following:

- (i) Article 1 number 2 of Law Number 4 of 1979 on Child Welfare (Kesejahteraan Anak, "Child Welfare Law") stated that: "a child is a person who has not reached the age of 21 years and never married."; and
- (ii) Article 1 number 5 of Law Number 39 of 1999 on Human Rights (Hak Asasi Manusia, "Human Rights Law") stated that: "a child is any human being under the age of 18 (eighteen) years and unmarried, including a child still in the womb if it is in his/her best interest."
- (iii) Article 1 number 1 of Law Number 23 of 2002 on Child Protection (Perlindungan Anak) (as lastly amended by Law Number 35 of 2014 and Law Number 17 of 2016 regarding the stipulation of Government Regulation in Lieu of the Law Number 1 of 2016, "Child Protection Law"), stated that: "a child is someone who hasn't reached the age of 18 years, including those who are still in the womb."
- (iv) Article 1 number 4 of Law Number 44 of 2008 on Pornography (Pornografi, "Pornography Law") stated that: "a child is a person who has not reached the age of 18 years."
- (v) Article 1 number 3, 4 and 5 of Law Number 11 of 2012 on Juvenile Justice System (Sistem Peradilan Anak) (as amended, "Juvenile Justice System Law") in defining the following terms stated that:
 - 1) a Child in Conflict with the Law is: "a child who is 12 years old, but not yet 18 (eighteen) years old who is suspected of committing a criminal offense";
 - 2) a Child Victim of Crime is: "a child under the age of 18 (years who experiences physical, mental, and/or economic loss caused by a criminal offense";
 - 3) a Child Witness to a Crime is: "a child under the age of 18 years who can provide information for the purpose of investigation, prosecution, and examination in court about a criminal case that such child has heard, seen, and/or experienced",



(vi) Article 1 number 5 of Law Number 12 of 2022 on Sexual Violence Crimes (“Sexual Violence Crimes Law”) stated that: “a child is someone who has not reached 18 (eighteen) years old, including children who are still in the womb.”

Besides the above, the Article 330 Indonesian Civil Code (Kitab Undang-Undang Hukum Perdata) also recognizes that minors are those who have not yet reached the age of 21 years and have not previously married.

It could be understood based on the several provisions in the aforementioned laws and regulations, there is still no uniformity regarding the age of adulthood or a child in Indonesia, where some give a limit of 21 (twenty-one) years, some are 18 (eighteen) years old, and even 17 (seventeen) years old (i.e., the age where one could start/count to vote pursuant to Regulation of General Election Commission (Peraturan Komisi Pemilihan Umum, “PKPU”) Number 7 of 2022 as lastly amended by PKPU Number 7 of 2023.

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>)

According to the explanation of Article 66 of Child Protection Law, Child Sexual Exploitation is: “any form of exploitation of a child's sexual or other organs for profit, including but not limited to only prostitution and sexual abuse.”

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

Sexually Explicit Conduct is not specifically defined in any of Indonesian laws and regulations. However, the Pornography Law defines “pornography” as images, sketches, illustrations, photos, texts, sounds, videos, animations, cartoons, conversations, gestures, or other form of messages via communication media and/or public performance, which contain obscenity or sexual exploitation in violation of public decency norms.

Further, Article 4 (1) of Pornography Law states that:

“Every person is prohibited from producing, making, reproducing, duplicating, disseminating, broadcasting, importing, exporting, offering, trading, renting, or providing pornography that explicitly contains:

- a. intercourse, including deviant intercourse;
- b. sexual violence;
- c. masturbation [...];
- d. nudity or the appearance of nudity;
- e. genitals; or
- f. child pornography.”

Additionally, Article 4 (2) of Pornography Law also sets that:

“Every person is prohibited from providing pornographic services that:

- a. explicitly presents nudity or the appearance of nudity;
- b. explicitly presents the genitals;
- c. exploits or exhibits sexual activity; or
- d. offers or advertises, either directly or indirectly, sexual services.”



Furthermore, Article 282-283 of the Indonesian Criminal Code also prohibits the conducts of offering, giving away continuously or temporarily, broadcasting, performing or pasting, handing over or displaying writings, images or objects that violate decency (*kesusilaan*), that may also include sexually explicit conduct. Article 533 of Indonesian Criminal Code also sets that:

“Shall be punished by a maximum light imprisonment of two months or a maximum fine of three thousand rupiahs:

1. any person who at a place of public traffic openly exhibits or puts up a writing with a title, cover or contents made legible, as well as a drawing or an object, capable of arousing the passions of the youth;
2. any person who at a place of public traffic openly plays out the contents of a writing capable of arousing the passions of adolescents;
3. any person who openly or unsolicited offers a writing, drawing or article capable of arousing the passions of juveniles, or openly or by broadcasting a writing in unsolicited manner designates as available a writing or drawing capable of arousing the passions of juveniles;
4. any person who offers, hands over permanently or temporarily, delivers or shows such pictures or objects to a minor under the age of seventeen years;
5. any person who plays out the contents of such writings in the presence of a minor under the age of seventeen years under the age of seventeen years.”

The “decency” element is not defined under any laws and regulations. Thus, the interpretation of this element may vary between different society groups and may change from time to time.

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

Child Sexual Abuse is not specifically defined in any of Indonesian laws and regulations. However, despite of the definition not being explicitly set, Child Sexual Abuse still falls/regulated under several of Indonesia regulations, for example, Article 15 of Child Protection Law stated that every child has the right of protection from sexual crimes (*kejahatan seksual*). Additionally, Sexual Violence Crimes Law also sets out the acts considered as Sexual Violence Crimes, which are also be applicable for child victims:

- (a) non-physical sexual harassment;
- (b) physical sexual harassment;
- (c) forced contraception;
- (d) forced sterilization;
- (e) forced marriage;
- (f) sexual abuse;
- (g) sexual exploitation;
- (h) sexual slavery; and
- (i) electronic-based sexual violence.

Further to the above, Article 4 (2) of Sexual Violence Crimes Law written that Sexual Violence Crimes shall also include:

- (a) rape;
- (b) lewd acts;
- (c) sexual intercourse with children, obscene acts against children, and/or sexual exploitation of children;



- (d) indecency acts that are contrary to the will of the Victim;
- (e) pornography involving children or pornography that explicitly contains sexual violence and exploitation;
- (f) forced prostitution;
- (g) human trafficking intended for sexual exploitation;
- (h) sexual violence in the household scope;
- (i) money laundering in which its original crime was a Sexual Violence Crime; and
- (j) other criminal acts that are expressly stated as Sexual Violence Crimes as regulated under the laws and regulations.

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

According to Article 4 (1) of Pornography Law, child pornography is: “any form of pornography involving children or involving adults who act or behave like children.”

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>)

Whilst Indonesian laws and regulations do not provide a specific definition for computer generated images or videos of child pornography/scam (either created by artificial intelligence or morphed), this type of images or videos would fall under the definition of “Electronic Information” and “Electronic Document” under Law Number 11 of 2008 on Electronic Information and Transaction/Informasi dan Transaksi Elektronik as recently amended by Law Number 1 of 2024 (“EIT Law”).

According Article 1 number 1 of EIT Law, Electronic Information is: “one or a set of electronic data, including but not limited to text, voice, image, map, design, photo, electronic data interchange (EDI), electronic mail, telegram, telex, telecopy or the like, letter, sign, number, Access Code, symbol, or perforation which has been processed and which has meaning or may be understood by people who are able to understand it.”

Additionally, pursuant to Article 1 number 4 of EIT Law, Electronic Document is: “any Electronic Information that is made, forwarded, transmitted, received, or stored in analog, digital, electromagnetic, optical, or similar format, and which may be seen, displayed and/or heard through a Computer or an Electronic System including but not limited to text, voice, image, design map, photo or the like, letter, sign, number, Access Code, symbol, or perforation which has meaning or definition or may be understood by people who are able to understand it.”

Both terms above are broadly defined, and therefore can include system-generated images/videos, including those that may be related to child pornography or CSAM.

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>)

Article 76E of Child Protection Law has set that: “Every person is prohibited from committing



Violence or threat of Violence, forcing, deceiving, committing a series of lies, or inducing a Child to commit or allow obscene acts to be committed.” Article 76I also stipulates that: “Every person is prohibited from placing, allowing, committing, ordering to commit, or participating in the economic and/or sexual exploitation of children.”

Moreover, Article 4 (2) of Sexual Violence Crimes Law (see section ‘d. Child Sexual Abuse’ above) also considered the act of sexual intercourse with children, obscene acts against children, and/or sexual exploitation of children as Sexual Violence Crimes.

In this regard, Article 417 Law Number 1 of 2023 on Indonesian Criminal Code/Kitab Undang-Undang Hukum Pidana (“New Indonesian Criminal Code”) regulates that: “Every person who gives or promises to give a gift, abuses the authority arising from a relationship of circumstances or by misleading a person who is known or reasonably suspected to be a child, to commit obscene acts or to allow obscene acts to be committed against them, shall be punished with a maximum imprisonment of 9 (nine) years.”

Additionally, Article 422 of the New Indonesian Criminal Code also sets that:

- “(1) Every person who moves, brings, places, or delivers a Child to another person to commit obscenity, prostitution, or other acts that contradict decency, shall be punished with a maximum imprisonment of 9 (nine) years.
- (2) If the crime as referred to in paragraph (1) is committed by promising the Child a job or other promises, shall be punished with a maximum imprisonment of 10 (ten) years.”

However, it should be noted that such New Indonesian Criminal Code will only take effect as of 2 January 2026.

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

Simply based on the Indonesian Criminal Code, the legal age of consent for sexual activity is 15 years old.

In this regard, Article 287 (1) Indonesian Criminal Code also states that: “Any person who has sexual intercourse with a woman outside of marriage, knowing or reasonably suspecting that she has not yet reached the age of fifteen years or, if her age is not obvious, that she is not yet marriageable, shall be punished by a maximum imprisonment of nine years.”

However, Article 76E Child Protection Law criminalizes anyone who persuades children to engaging in an obscene activity. Further, Article 6 letter c of Sexual Violence Crimes Law also criminalizes anyone who abuses their position, authority, trust, or character based on deceit, circumstances or vulnerability, inequality, or dependency, to force or deceptively influencing another person to engage in a sexual activity or engaging in an obscene activity.

Thus, as individuals under the age of 15 are considered as children, theoretically, engaging in sexual activity (even based on consent) could still be criminalized, as this could be persuading children to engage in criminal activity based on abusing circumstances or vulnerability.

Regarding the definition of a child pursuant to the Sexual Violence Crimes Law and Child



Protection Law (see section 'a. Child or Minor' above), it is also supported by Article 14 (5) of Sexual Violence Crimes Law that states in the event that a victim is a child or a person with disability, the existence of the will or consent of the victim does not eliminate criminal charges for sexual violence crimes using electronic systems.

- 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>)**

Sextortion is not specifically defined in any of Indonesia's laws and regulations. However, act of sextortion may fall under the form of the following acts of Sexual Violence Crimes according to Article 4 of Sexual Violence Crimes Law:

- (i) sexual exploitation;
- (ii) force of prostitution;
- (iii) sexual intercourse with children, obscene acts against children, and/or sexual exploitation of children; and
- (iv) pornography involving children or pornography that explicitly contains sexual violence and exploitation.

Additionally, pursuant to Article 14 (1) – (2) of Sexual Violence Crimes Law, it is also stated that:

- “(1) Any Person who without right:
- a. recording and/or taking pictures or screenshots of sexual content against the will or without the consent of the person who is the object of the recording or picture or screenshot;
 - b. transmits electronic information and/or electronic documents that are sexually charged against the will of the recipient that are directed towards sexual desires; and/or
 - c. stalking and/or tracking using an electronic system of the person who is the object of the electronic information/document for sexual purposes, shall be punished for committing electronic-based sexual violence, with a maximum imprisonment of 4 (four) years and/or a maximum fine of IDR200,000,000.00 (two hundred million rupiah).
- (2) In the event that the act as referred to in paragraph (1) is committed with the intent:
- a. to commit extortion or threaten, force; or
 - b. mislead and/or deceive, someone to do, let be done, or not to do something, shall be punished with a maximum imprisonment of 6 (six) years and/or a maximum fine of IDR300,000,000.00 (three hundred million rupiah).”

Additionally, pursuant to the explanation of Article 66 of Child Protection Law, it could be understood that economically exploited child are children who are victims of, including but not limited to, extortion, slavery, oppression, physical, sexual, reproductive organ exploitation, or the use of the child's power or ability by other parties for material gain. Economically exploited children itself is protected with one of the provisions as stipulated in Article 76I of Children Protection Law

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

In general, Electronic System Operators (“ESO(s)”), including Online Platform operators, are required under the regulations to ensure that their electronic systems neither contain prohibited content nor facilitate the distribution of prohibited content. This obligation is expressly stipulated under Government Regulation Number 71 of 2019 on the Operation of Electronic Systems and Transactions (“GR 71/2019”) Electronic System Providers in Indonesia Minister of Communication and Informatics Regulation Number 5 of 2020 on Private Scope Electronic System Operator, as amended by the Minister of Communication and Informatics Regulation Number 10 of 2021 (“MoCI Reg. 5/2020”).

Prohibited content referred to above is classified into the following categories:

- 1) a violation of the laws and regulations;
- 2) causes public unrest or disturbance of public order; and
- 3) provides advice on how to access or provides access to prohibited content.

Considering that child pornography and CSAM content is considered as violating the laws and regulations (such as the Pornography Law, Child Protection Law, and Sexual Violence Crimes Law); thus, Online Platform operators must implement measures to prevent and delete these types of content from distribution in their platform.

As the regulations do not specify the specific measures to comply with the above requirement, it could be interpreted that ESOs may implement any measures, to the extent that these measures would allow ESOs to entirely remove and prevent prohibited content being distributed on their platform. In practical terms, we view that this could only be achieved by implementing the following measures:

- 1) establishing a user policy, terms and conditions, and/or guidance, which clearly prohibits the creation, distribution, sharing, displaying, or provision of access to prohibited content;
- 2) implementing a monitoring mechanism (either by human or automated) to detect prohibited content;
- 3) implementing a filtering mechanism to automatically detect and prohibit the creation, distribution, sharing, displaying, or provision of access to prohibited content;
- 4) providing a reporting mechanism for the public to report any prohibited content in the platform; and
- 5) taking down prohibited content based on self-discovery, report from the public, or report from the authority.

b. review, screen, moderate, or detect content to identify enticement, grooming, or sextortion of a child

Similarly, to the response in point (a), online platforms, which are classified as ESOs, are obligated to ensure that their electronic systems neither contain prohibited content nor facilitate the distribution of prohibited content. Considering that enticement, grooming, and sextortion of a child is prohibited under Article 76E of Child Protection Law affirms that engaging in violence, coercion, deception, spreading falsehoods, or encouraging obscene



acts, especially involving children, is strictly prohibited. Thus, the prohibition of enticement and grooming of children under Indonesian law is to safeguard the well-being, safety, and rights of minors. Sextortion is not explicitly defined in Indonesian Law. Albeit, it may be categorized under Article 4 of the Sexual Violence Crimes Law, encompassing sexual exploitation, forced prostitution, sexual acts involving children, obscene acts against children, and child pornography, including explicit depictions of sexual violence and exploitation. Therefore, Online Platforms must implement content review, screening, moderation, and detection mechanism to prevent these contents from distribution.

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

The laws and regulations do not expressly require Online Platform to report to the government agency or nongovernmental organization upon discovering child pornography, CSAM, enticement, grooming, or sextortion content. However, theoretically, if an Online Platform operator does not enforce content removal, account blocking, and/or reporting the existence of these type of content, the platform operator could be deemed as engaging in the following crime:

- 1) placing, allowing, committing, ordering to commit, or participating in the economic and/or sexual exploitation of a child, which is subject to imprisonment up to 10 years and/or fine up to IDR 200,000,000.00, as regulated under Article 76I and Article 88 of Child Protection Law;
- 2) anyone who, without rights and with the intent to extort, threaten, coerce, mislead, or deceive, records, captures images, or takes screenshots containing non-consensual sexual content; transmits such content against the recipient's will for sexual purposes; or engages in stalking or tracing using electronic systems for sexual purposes, is liable for electronic-based sexual violence. The maximum penalty for this offense is imprisonment for up to 4 years and/or a fine of up to IDR 200,000,000.00 under Article 14 (1) of Sexual Violence Crimes Law.
- 3) unauthorized broadcasting, showing, distributing, transmitting, or making accessible of electronic information/documents with indecent or gambling content is prohibited. Offenses related to decency or sexual exploitation of children will be aggravated by one-third of the basic punishment in such cases, as stipulated under Articles 27 (1) and 52 (1) of EIT Law.
- 4) anyone financing or facilitating the production, reproduction, dissemination, broadcasting, import, export, offer, sale, rental, or provision of explicit pornography, as mentioned, may face imprisonment ranging from 2 to 15 years and/or a fine ranging from at least IDR 1,000,000,000.00 to a maximum of IDR 7,500,000,000.00 as stipulated under Article 33 of L Pornography Law.

There is no specific regulation in Indonesia governing the requirement for Online Platforms to report CSAM, Enticement, Sexual Grooming, or Sextortion, nor is it mandated for these platforms to notify Law Enforcement or NGOs within their systems. Instead, their obligation is limited to providing reporting facilities. According to MoCI Reg. 5/2020, electronic system providers in both the public and private sectors are obligated to offer reporting facilities. Through these facilities, the public can submit complaints and/or reports regarding prohibited Electronic Information and/or Electronic Documents within the Electronic System they manage. In addition, under Article 66 Child Protection Law, provides that there is special



protection for Children who are economically and/or sexually exploited, in which actions as explained below should be implemented:

- 1) Dissemination and/or socialization of the provisions of laws and regulations relating to the protection of children who are economically and/or sexually exploited;
- 2) Monitoring, reporting, and sanctioning; and
- 3) Involvement of various companies, labour unions, non-governmental organizations, and society in the elimination of economic and/or sexual exploitation of children. sexual exploitation.

Nevertheless, the MoCI has established an Online Platform where anyone can report these issues. Reports on such matters can be submitted through aduankonten.id or sent via email to MITC at aduankonten@kominfo.go.id. It should be emphasized that Indonesia's existing legal framework is limited to addressing the consequences of engaging in sexual grooming, child pornography, and sextortion. The laws govern the consequences related to sexual grooming and sextortion, with penalties determined by the severity of the misconduct.

d. remove or take down any child pornography, CSAM, enticement, grooming, or sextortion that they identify, become aware of, or are notified about

According to Article 13 MoCI Reg. 5/2020, Online Platforms are required to take down electronic information and/or electronic documents that:

- 1) violate the provisions of laws and regulations;
- 2) disturbing the public and disturbing public order; and
- 3) informing how to or providing access to prohibited electronic information and/or electronic documents.

Given that content involving child pornography, CSAM, enticement, grooming, or sextortion is prohibited by Pornography Law, Online Platforms are obligated to remove such content. Such mechanism is provided by Article 15 MoCI Reg. 5/2020 where, MoCI will issue a takedown request to the ESO to take down the prohibited content. The Electronic System Operator in question must take down the said content within 4 hours upon receipt of the takedown request.

Failure to comply with the takedown request is subject to administrative sanction of fine, which will be calculated based on a certain formula (which considers the type of content, the ESO's compliance level, virality of the content, etc.) up to access blocking to the ESO's platform.

e. review content by human moderators to screen or moderate for child pornography or CSAM

Under existing laws and regulations, there is no specific provision that directly regulates Online Platforms to employ human moderators for the screening or moderation of child pornography or CSAM. According to Article 9 (3) of Ministry of Communication and Informatics Regulation Number 5/2020, Private Scope ESOs are obligated to ensure that their electronic systems neither contain nor facilitate prohibited content. The regulation doesn't explicitly mandate the use of human moderators. ESOs have the flexibility to decide on the use of human moderators, provided that the implemented mechanism effectively remove and prevents the distribution or facilitation of prohibited content in their electronic systems.



- 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**

Online platforms' removal of content distribution is regulated under MoCI Reg. 5/2020, based on a takedown mechanism elaborated in point d above.

The institution authorized to issue a takedown request is the MoCI. Thus, theoretically, Online Platforms are only required to comply with a takedown request from the MoCI.

However, the MoCI can receive a request for the issuance of a takedown request from the public (including society and nongovernmental organization), other ministries/institutions, law enforcement authorities, and judicial institutions, in which the MoCI will issue the official takedown request upon receiving and reviewing the request.

- 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.**

There is no particular regulation mandating Online Platforms to employ specific technology for the detection, removal, blocking, or takedown of child pornography, CSAM, enticement, grooming, or sextortion. However, there is an obligation under Article 9 (3) MoCI Reg. 5/2020 for ESOs to ensure that:

- 1) Its electronic system does not contain electronic information and/or electronic documents that are prohibited; and
- 2) its electronic system does not facilitate the dissemination of prohibited electronic information and/or electronic documents.

Thus, an Online Platform may or may not use hashing technology, to the extent they can ensure that their platform does not distribute or facilitate the distribution of prohibited content.

Moreover, there is no particular regulation mandating Online Platforms to employ specific technology for the detection, removal, blocking, or takedown of child pornography, CSAM, enticement, grooming, or sextortion. However, there is an obligation under Article 9 (3) MoCI Reg. 5/2020 for ESOs to ensure that:

- 1) its electronic system does not contain electronic information and/or electronic documents that are prohibited; and
- 2) its electronic system does not facilitate the dissemination of prohibited electronic information and/or electronic documents.

Thus, an Online Platform may or may not use AI or machine learning tools, to the extent

they can ensure that their platform does not distribute or facilitate the distribution of prohibited content.

- 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.?**

The abovementioned regulations are applicable to all Online Platform (regardless of their scale, number of users, or types of services), except that the obligation to provide a public reporting mechanism is mandatory for User Generated Content (UGC) platforms, as stipulated under Article 10 MoCI Reg. 5/2020. With regard to this requirement, online UGC platform operators must:

- 1) provide a response to the complaint and/or report to the complaining party and/or report;
- 2) conduct an independent examination of complaints and/or reports and/or request verification of complaints and/or reports to the Minister and/or related Ministries or Institutions;
- 3) provide notification to Electronic System Users regarding complaints and/or reports against Electronic Information and/or Electronic Documents that are reports on Electronic Information and/or Electronic Documents uploaded by Electronic System Users; and Electronic System User; and
- 4) rejecting complaints and/or reports if the Electronic Information and/or Electronic Document reported is not the Electronic Information and/or Electronic Document that is prohibited.

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?

Pursuant to Article 16A (1) of EIT Law, Electronic System Operators are obligated to provide protection for children who use or access the Electronic System. Specifically, the said protection includes protection of children's rights as intended in statutory regulations regarding the use of products, services and features developed and operated by Electronic System Operators.

Moreover, Electronic System Operators are required to implement technology and operational technical measures to provide protection as referred to in Article 16A (1) EIT Law from the development stage to the Electronic System Operation stage in providing products, services and features for children.

In this regard, Article 16A (4) EIT Law specifies that in order to provide protection as referred to in Article 16A (1) EIT Law, the Electronic System Operators are required to provide:

- a. information regarding the minimum age limit for children who can use the product or service;
- b. child user verification mechanism; and
- c. mechanism for reporting abuse of products, services and features that violate or have the potential to violate children's rights.

However, the legal framework to implement the Article 16A EIT Law is regulated to be provided through the government regulation, which has not been issued yet.

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?

In general, the protection for children in accessing electronic systems is governed by the EIT Law. Pursuant to Article 16 (4) of the EIT Law, to ensure child protection, Electronic System Providers must provide (i) information about the minimum age limits for children using their products or services, (ii) implement mechanisms to verify the identity of child users, and (iii) establish reporting mechanisms for any misuse of products, services, or features that may infringe upon or potentially violate the rights of children. However, this regulation does not encompass specific provisions regarding the obligation of parental approval for children to access electronic systems.

The implementation of Article 16A of EIT Law within the legal framework is intended to be established through government regulations. However, as of now, there is no government regulation specifically addressing parental consent requirement.

Meanwhile, according to Article 330 ICC, minors (those who are below 21 years or not previously married) are deemed as do not have the capacity to enter into a contract.

Thus, theoretically, Online Platforms are required to secure parental/guardian consent for users that are below 21 years. Although non-compliant with this requirement is not subject to any immediate sanction, there is a theoretical risk that any agreement established with minor users without parental/guardian consent would be subject to challenge before a court based on a claim from an interested party.

Separately, if the use of Online Platforms involves the processing of users' personal data, the requirements under Law Number 27 of 2022 on Personal Data Protection ("PDP Law") would apply. Pursuant to Article 25 of the PDP Law, the processing of a child's Personal Data must be carried out in a special implementation which is by obtaining approval from the child's parent and/or child's guardian. Currently, the PDP Law is silent on the specific definition of a 'child'.

However, the government is currently preparing a draft regulation on the implementation of the PDP Law, which is expected to define children as those who are below 18 years.

- 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?**

Pursuant to Article 26 of EIT Law, it is regulated that ESOs are obligated to:

- (i) delete the irrelevant electronic information and/or electronic documents that are under its control at the request of the person who is under its control. electronic information and/or irrelevant electronic documents under its control at the request of the person concerned based on a court order; and
- (ii) provide a mechanism for deleting Electronic Information and/or Electronic Documents that are no longer relevant in accordance with the provisions of the regulations. and/or Electronic Documents that are no longer relevant in accordance with the provisions of laws and regulations.

In connection with the said regard, Article 15 GR 71/2019 regulates that ESOs are obligated to delete irrelevant electronic information and/or electronic documents under its control at the request of the person concerned. In this regard, the obligation to delete irrelevant electronic information and/or electronic documents consists of:

- (i) deletion (right to erasure); and
- (ii) removal from search engine lists (right to delisting).

In addition to the above, Article 15 (1) of MoCI Reg. 5/2020 allows the public (including individuals) to file a request to the MoCI to issue a takedown request. Under this mechanism, the MoCI will issue an official takedown request to the relevant ESO, upon receiving and reviewing a request from the public.

Subsequently, the ESO in question must take down the prohibited content specified in the takedown request within a specific timeline (i.e., 24 hours for regular takedown request or 4 hours for urgent takedown request (related to terrorism, child pornography, and content disturbing public order)).

b. An obligation on the part of the Online Platform to take active steps to remove the pornography or other imagery from their servers?

In general, under GR 71/2019 and MoCI Reg. 5/2020, ESOs, are required to ensure that their electronic systems neither contain prohibited content nor facilitate the distribution of prohibited content. In connection to the said regard, pursuant to Article 13 MoCI Reg. 5/2020, Private ESOs are required to terminate access (take down) of electronic information and/or electronic documents that are prohibited as referred to in Article 9 (4) MoCI Reg. 5/2020. Moreover, the obligation to terminate access (take down) includes terminating access to electronic information and/or electronic documents that can facilitate the dissemination of prohibited electronic information and/or electronic documents.

Specifically, the scope of electronic information and/or electronic documents that must be taken down pursuant to Article 9 (4) MoCI Reg. 5/2020 includes:

- (i) violating the provisions of laws and regulations;
- (ii) disturbing the public and disrupting public order; and
- (iii) informing methods or providing access to prohibited electronic information and/or electronic documents.

Therefore, to ensure the compliance towards the abovementioned obligations, the online platforms are obligated to delete irrelevant electronic information and/or electronic documents under its control at the request of the person concerned as well as actively implement the official takedown request provided by MoCI as referred to in Article 15 (1) MoCI Reg. 5/2020.

c. An ability to get an injunction or other court order against the Online Platform to stop them from publishing the pornography or imagery?

There are several mechanisms, as follows:

1. Take Down Request through the Court or MoCI

The victim may request the court to obtain the order to take down the requested content pursuant to Article 26 (6) EIT Law. Otherwise, the victim may request the take down of pornography or CSAM imagery, pursuant to Article 15 (1) MoCI Reg. 5/2020 where, MoCI orders the Electronic System Operator to terminate access (take down) of prohibited contents.

Subsequently, the ESO in question must take down the prohibited content specified in the takedown request within a specific timeline (i.e., 24 hours for regular takedown request or 4 hours for urgent takedown request (related to terrorism, child pornography, and content disturbing public order)).

2. Tort Lawsuit

The ability to get an injunction or other court order against the Online Platform to stop them from publishing the pornography or imagery is principally being carried out through the tort lawsuit under the Article 1365 ICC which stipulates:

“Every unlawful act which causes damage to another obliges the person who caused the damage through his fault to compensate for the damage.”

Pursuant to the frequent practice, the unlawful act could be interpreted as to include violations of both statutory law and unwritten norms of law, such as propriety, customs, and reasonableness. This may include the act of publishing pornography or imagery through the Online Platform.

Moreover, considering that such conduct is being carried out in the electronic platform.

Article 38 EIT Law stipulates that:

- “(1) Every person may file a lawsuit against a party organizing an Electronic System and/or using Information Technology that causes harm.
- (2) The public may file a lawsuit on a representative basis against a party organizing an Electronic System and/or using Information Technology that results in harm to the public, in accordance with the provisions of the Laws and Regulations.”

However, referring to the current practice, to our knowledge, there is no lawsuit which has been carried out to the Online Platform to stop them from publishing certain contents.

Specifically, for pornography or imagery circulated on the internet. Please note that the Claimant/Plaintiff may request an injunctive relief (such as cease and or desist order) in form of interlocutory decision and or final decision to be issued by the Court to compel the Online Platform to stop publish of the pornography or imaginary.

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?

A protective order may be requested through the tort lawsuit which carried out under Article



1365 ICC. This provision stipulates that every unlawful act which causes damage to another obliges the person who caused the damage through his fault to compensate for the damage.

In this regard, the compensation of damages under 1365 ICC may be provided in form of prohibition in carrying out certain action. Therefore, the victim may request the tribunal to render the judgement to prohibit the perpetrator to post pornography or imagery in the future on the same or other online platform.

However, referring to the current practice, to our knowledge, there is no lawsuit which rendered the judgment to prohibit the losing party to post pornography or imagery 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?

Under the prevailing laws and regulations in Indonesia, the ability to seek financial damages or any sort of monetary recovery from an offender may be carried out through the following mechanisms:

(i) Tort Lawsuit through Civil Proceeding

The tort lawsuit may be carried out pursuant to Article 1365 ICC which stipulates that every unlawful act which causes damage to another obliges the person who caused the damage through his fault to compensate for the damage. In this regard, the said damage may include any monetary recovery.

The unlawful act could be interpreted as to include violations of both statutory law and unwritten norms of law, such as propriety, customs, and reasonableness. Therefore, it may include the act of sharing child's image or video without consent.

(ii) Restitution within Criminal Proceeding

Pursuant to Article 1 Number 20 of Sexual Violence Crimes Law, restitution is the payment of compensation charged to the perpetrator or third party based on a court stipulation or judgement that has permanent legal force, for material and/or immaterial losses suffered by the victim or his heirs.

Subsequently, under Article 30 Sexual Violence Crimes Law, victims of crimes of sexual violence have the right to receive restitution in the form of:

- a. compensation for loss of wealth or income;
- b. compensation for losses incurred as a result of suffering directly related to the crime of sexual violence;
- c. reimbursement for medical and/or psychological care; and/or
- d. compensation for other losses suffered by the victim as a result of the crimes of sexual violence.

In this regard, under Article 16 (1) Sexual Violence Crimes Law, the judges are obliged to determine the amount of restitution for crimes of sexual violence which are punishable by imprisonment of 4 (four) years or more.

The mechanism of restitution further regulated under:

- a. Law Number 13 of 2006 on the Protection of Witnesses and Victims as recently amended by Law Number 31 of 2014 (“Law 13/2006”) as implemented through Government Regulation Number 7 of 2018 on the Provision of Compensation, Restitution and Assistance to Witnesses and Victims as recently amended by Government Regulation Number 35 of 2020 (“GR 7/2018”); and
- b. In the event the victims are children, the mechanism is specifically regulated under Law Number 23 of 2002 on Child Protection as recently amended by Law Number 17 of 2016 as implemented through Government Regulation Number 43 of 2017 on the Implementation of Restitution for Children Who Are Victims of Crime (“GR 43/2017”).

Pursuant to Article 71D Child Protection law, every child who is a victim of pornography shall have the right to apply to the court in the form of restitution. In this regard, under Article 5 and 6 GR 43/2017, the restitution may be submitted through the following mechanism:

- (i) Submitted before the stipulation of the court judgement

The restitution shall be submitted through the stage of investigation or prosecution. Otherwise, it may be submitted through Witness and Victim Protection Agency/Lembaga Perlindungan Saksi dan Korban (LPSK).

- (ii) Submitted after the stipulation of the court judgement

The restitution shall be submitted after the court judgement has obtained permanent legal force. In this regard, LPSK shall submit an application to the court to obtain the court decision for the said restitution

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?

Under Sexual Violence Crimes Law, it can be argued that the victim monetary compensation would primarily be provided through restitution as referred to in Article 30 Sexual Violence Crimes Law. However, Article 35 Sexual Violence Crimes Law regulates that in the event that the perpetrator’s confiscated assets are insufficient to be used as restitution, the state shall provide compensation for the underpayment of restitution to the victim in accordance with the court judgement. Specifically, the compensation shall be provided through the “victim assistance fund”, which can be defined as the state compensation fund for victims of crimes of sexual violence.

Apart from the abovementioned monetary compensation, there are several rights for the victim regulated under Government Regulation Number 78 of 2021 on the Special Protection for Children (“GR 78/2021”). Pursuant to Article 3 GR 78/2021, the central government, regional governments, and other state institutions are obliged and responsible for providing special protection to child victims of pornography. In this regard, the special protection for children is carried out through:

- (i) rapid treatment, including physical, psychological, and social treatment and

- rehabilitation, as well as prevention of disease and other health problems;
- (ii) psychosocial assistance during treatment until recovery;
- (iii) provision of social assistance for children who come from poor families; and
- (iv) provision of protection and assistance in every judicial process.”

Specifically, for the Child Victims of Pornography, Article 28 GR 78/2021 stipulates that special protection for children who are victims of pornography shall be implemented through counselling, mentoring, and social, physical and mental health recovery efforts.

Moreover, Article 34 GR 78/2021 stipulates that:

- (i) counselling and mentoring shall be carried out by the minister, the minister who organizes government affairs in the field of religion, and the regional government in accordance with their authority; and
- (ii) social recovery, physical and mental health shall be carried out by the minister who organizes government affairs in the social sector and the minister who organizes government affairs in the health sector.

g. notification to a victim when an offender is arrested for distributing child pornography or CSAM in which the child is depicted?

Pursuant to Article 10 (5) Head of The State Police Regulation Number 6 of 2019 on the Criminal Investigations (“Police Reg. 6/2019”), the investigator of criminal cases must issue the Notification Letter on the Progress of Investigation Results/Surat Pemberitahuan Perkembangan Hasil Penyidikan (“SP2HP”) for every development of case handling in criminal investigation activities. In this regard, pursuant to Article 1 number 17 Police Reg. 6/2019, SP2HP is a notification letter to the reporter/complainant regarding the progress of the investigation.

Therefore, the victim (as the complainant) may be notified by the investigator when an offender is arrested for distributing child pornography or CSAM in which the child is depicted through the SP2HP.

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?

In Indonesia, there is currently no specific regulation that dictates the precise concept of safety by design or safety measures each Online Platform must implement. Nevertheless, GR 71/2019 addresses aspects of safety measures that must be considered in organizing Electronic Systems. While there is a no explicit directives for safety measures on individual Online Platforms, GR 71/2019 provides a broader regulatory framework highlighting safety considerations for the operation of Electronic Systems in the country.

Article 3 (1) and (2) of GR 71/2019 stipulates that:

- “(1) Any Electronic System Provider shall organize Electronic System in a reliable and safe manner as well as be responsible for the proper operation of the Electronic System.
- (2) The Electronic System Provider shall be responsible for the organization of its

Electronic Systems.”

Furthermore, Article 5 of GR 71/2019 stipulates that:

- “(1) The Electronic System Provider must ensure that their Electronic System does not contain Electronic Information and/or Electronic Document which are prohibited in accordance with laws and regulations.
- (2) The Electronic System Provider must ensure their Electronic System does not facilitate the dissemination of prohibited Electronic Information and/or Electronic Document in accordance with laws and regulation.
- (3) The provision on the obligation of the Electronic System Provider as referred to in paragraph (1) and paragraph (2) shall be regulated with Regulation of the Minister.”

Pursuant to the Article 5 (3) GR 71/2019 above, Article 9 (4) MoCI Reg. 5/2020 has been issued and governs that prohibited information, specifically Electronic Information and/or Electronic Documents, classified as follows:

- (i) violating the provisions of laws and regulations;
- (ii) disturbing the public and disrupting public order; and
- (iii) notifying methods or providing access to prohibited Electronic Information and/or Electronic Documents.

Article 13 of GR 71/2019 stipulates that: “The Electronic System Provider shall own a governance policy, operation work procedures, and mechanism for audit which is conducted periodically to the Electronic System.”

Although there is no specific regulation specifying particular safety measures each Online Platform must adopt, besides GR 71/2018, MoCI Reg. 10/2021 also addresses crucial safety aspects concerning prohibited content. This regulation imposes mandatory measures to ensure that platforms neither host nor facilitate the distribution of prohibited content, as stipulated in Article 9 (3) MoCI Reg. 10/2021:

- “(3) Private Electronic System Providers are obliged to ensure that:
 - a. Their Electronic Systems do not contain prohibited Electronic Information and/or Electronic Documents; and
 - b. Their Electronic Systems do not facilitate the dissemination of prohibited Electronic Information and/or Electronic Documents.”

i. If so, must these steps be taken before the launch of an Online Platform?

Theoretically, in order to ensure utmost compliance with the regulations, every platform operator must adopt the above steps before making their Online Platform available in Indonesia or to Indonesian users.

ii. If so, if an Online Platform has already been in public use, when must they have incorporated “Safety by Design” measures?

In the event that an Online Platform has already been in public use, the safety measures mentioned previously shall immediately make an adjustment to ensure compliance with the regulatory requirements. Any necessary adjustments the initial launch of the Online Platform should be immediately executed, including taking down prohibited Electronic Information and/or

Electronic Document.

- iii. **For each of 6(a)(i) or (ii) above, please describe the legal requirement or recommendation.**

The legal requirements of “Safety by Design” incorporation before or after an Online Platform has been launched to public is also regulated under Chapter III Article 9 MoCI Reg. 5/2020. With the Private Scope ESO is responsible for the implementation of the Electronic System and the management of Electronic Information and/or Electronic Documents in the Electronic System reliably, securely, and safely. Therefore, an ESO must have a sufficient management system so that careful supervision can be carried out including providing access to relevant stakeholders, reporting facilities which is accessible to public and subject to take down provisions.

- 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”?**

There is no specific regulation that stipulates the exact parameters for monitoring, management, and enforcement for the Online Platform’s incorporation of “Safety by Design”, as long as it fulfils the obligations in MoCI Reg. 5/2020 to ensure that the platform does not host and does not facilitate the distribution of prohibited content. While specific detail on monitoring, management, and enforcement are not regulated, platforms should adopt measures that effectively fulfil these requirements, making sure they follow the rules laid out in MoCI Reg. 5/2020.

To do this, Online Platforms should establish technical and organizational instruments aligned with the principles of MoCI Reg. 5/2020. This approach ensures that platforms fulfil their legal obligations in accordance with Indonesian regulations governing ESO.