GLOBAL LEGAL INSIGHTS

AI, Machine Learning & Big Data 2026

Eighth Edition

Contributing Editor:
Charles Kerrigan
CMS LLP

glg Global Legal Group

TABLE OF CONTENTS

Indonesia

Abadi Abi Tisnadisastra
Prayoga Mokoginta
Aloysius Andrew Jonathan

ATD Law in association with Mori Hamada

1. Trends

1.1 General trends of AI use in Indonesia

Indonesia has witnessed accelerating adoption of artificial intelligence ("**AI**"), machine learning, and big data analytics (jointly referred to as "**AI and Data-Driven Technologies**") across multiple sectors of the economy. Across various reports/publications, businesses that have implemented AI solutions report notable increases in revenue and meaningful cost savings. This increasing trend is driven by the country's large population and growing digital economy.

In recognition of this trend, various government-led initiatives have been introduced in the past few years – ranging from a ministerial white paper on AI development and ethical guidelines for the use of AI, to plans for a specific regulation for the use of AI – primarily to outline Indonesia's general vision and macro-policy for AI and Data-Driven Technologies. As further discussed in section 5 "Regulations/government intervention" below, a Presidential Regulation on AI ("**AI Presidential Regulation**") is expected to be promulgated to establish a more comprehensive – and standalone – AI legislation in Indonesia; the issuance date of which has not yet been confirmed.

1.2 Government roadmap and initiatives on AI and Data-Driven Technologies

Various government authorities have published a roadmap and initiatives that set out its views and general direction on the expected role and regulation of AI and Data-Driven Technologies:

- Agency for the Assessment and Application of Technology's Indonesian Artificial Intelligence National Strategy 2020–2045. This strategy identified the priority sectors for AI implementation, namely: healthcare; bureaucratic reform; education and research; food security; and mobility and smart cities. Key challenges in AI adoption include the dominance of imported technologies' potential to cause disruptions to the workforce, and risks of data misuse.
- Indonesia Financial Service Authority's ("**OJK**") Artificial Intelligence Governance for Indonesian Banking 2025. OJK considers that the adoption of AI is highly beneficial for the banking sector, with use case examples for processing documents, risk management, fraud detection, customer service, etc. On the other hand, OJK considers the challenges of AI use against the banking sector to include new

methods for fraud (e.g., using AI to impersonate key persons, customers, etc.), bias and inaccuracies of AI (especially if implemented for credit risk functions), new avenues of cybersecurity risks, and human issues in the use of AI (e.g., leadership and policy familiarity). OJK outlines that the core values to realise responsible and trustworthy AI include reliability, accountability and human oversight.

- Ministry of Communications and Digital's ("**MOCD**") AI Roadmap White Paper. This roadmap was developed collaboratively by the AI Roadmap Task Force, comprising 443 members representing government, academia, industry, civil society organisations, and media, and outlines AI development priorities, financing, and ethical guidelines and regulations.

Aside from roadmaps, the Indonesian government has also shown some early initiatives in the realm of AI governance, which still has its focus on ethical governance. For instance, in late 2024, the Ministry of Communications and Informatics (now called the MOCD) completed the AI Readiness Assessment for Indonesia using UNESCO's Readiness Assessment Methodology. This step marks Indonesia as the first country in Southeast Asia to do so. It evaluates Indonesia's AI landscape across five dimensions: legal and regulatory; socio-cultural; economic; scientific and educational; and technological and infrastructural. The assessment identified several key areas for improvement, including economic and socio-cultural impacts, AI-associated risks, and research funding gaps compared to neighbouring countries.

The Indonesian government has also been planning several draft regulations on the development and governance of AI. Several non-binding guidelines on the use of AI have been issued by different government authorities. These items will be further touched upon in section 5 "Regulations/government intervention" below.

2. Ownership/protection matters related to AI and Data-Driven Technologies

2.1 IP-related protection

The current Indonesian intellectual property ("**IP**") framework presents significant challenges and gaps when applied to AI and AI-produced works, as most legal frameworks were designed before the widespread adoption of AI and Data-Driven Technologies. Although most IP regulatory frameworks have not specifically adopted AI and Data-Driven Technologies, existing guidelines and non-binding circular letters on AI have specially mentioned that the protection of IP is a fundamental principle in the operation and development of AI (as further discussed in section 5 "Regulations/government intervention" below).

Copyright and AI

Within the realm of the IP regulatory regime, copyright laws and regulations may intersect significantly with AI and AI-produced works.

In terms of the AI tool (the software), the computer/source code that implements the AI can be protected by copyright under Law No. 28 of 2014 on Copyright, as amended ("**Copyright Law**") as a computer program. By contrast, the underlying "algorithm" shall not be protected by copyright, as it falls under an abstract idea, method, or procedure – i.e., works that are not copyrightable even if they are described or embedded in a copyrightable work.

Similarly, assessing whether AI-generated content/work can be protected under copyright will also not be as straightforward. Under the Copyright Law, a work must be: (i) created by a person or persons; and (ii) distinct/original. In this regard, it remains unclear whether AI-generated works can be accorded copyright protection, particularly due to the level of human input (or lack thereof) in generating the works.

Trademarks and AI

Law No. 20 of 2016 on Trademark and Geographical Indications, as amended does not have any specific restriction or provision that addresses AI and its generated work. Specifically, a trademark that can be

registered and protected in Indonesia is a two- and/or three-dimensional image/logo/words/numbers/colours that must have the ability to be able to distinguish certain goods and/or services. Accordingly, provided that works produced by AI satisfy these requirements, they may theoretically be eligible for trademark registration, subject to not infringing upon existing trademarks.

Patents and AI

Indonesian patent law, i.e., Law No. 13 of 2016, underwent its third amendment in 2024 through Law No. 65 of 2024 (together, the "**Patent Law**"). The 2024 amendment introduces systems, methods, and uses as part of "inventions". However, the Patent Law maintains its core requirements regarding patentability (i.e., novelty, inventive step, and industrial applicability) and inventorship (human involvement).

Other IP-related issues in terms of AI tools and AI-produced works

Ownership of AI source code and technology

- Under the Copyright Law, the creator of a work is in principle the copyright holder. In an employment context (for the creation of AI source code), it is important for the employment agreements to clearly state that all economic rights in works created within the scope of employment are assigned to the company.
- Where AI development is undertaken by external vendors, consultants, or contractors, the commissioning company may not automatically own the resulting IP unless there is a proper written assignment or work-for-hire arrangement in the underlying agreement.
- Collaborative AI development involving multiple parties without clear contractual allocation of IP rights may lead to disputes over ownership, commercialisation rights, and licensing entitlements.

Copyright concerns in AI training inputs and outputs

- Under the Copyright Law, using copyrighted material without permission constitutes copyright infringement, particularly for commercial purposes. While limitations exist for non-commercial uses such as education and research, these would not extend to commercial AI training or large-scale data mining.
- Input stage risks: Developers of AI tools need to ensure that datasets used for training models do not result in copyright infringement. This includes verifying that training data is properly licensed, in the public domain, or otherwise lawfully obtained.
- Output stage risks: Risk of copyright infringement may still arise if AI-generated content shares substantial similarities with pre-existing copyrighted works, potentially constituting reproduction, adaptation, or derivative work without authorisation.

Web scraping and digital content use

- Given the ability of AI tools to conduct web searches and scrape online articles, additional IP considerations arise in the digital context, particularly regarding reproduction and use of third-party content.
- Presidential Regulation No. 32 of 2024 on Responsibilities of Digital Platform Companies on Quality Journalism ("**PR 32/2024**" – which will be further discussed in section 5 "Regulations/government intervention" below) touched upon publishers' rights to obtain compensation from digital platforms (broadly defined, which may include those digital platforms that operate AI tools) that utilise their content.

2.2 Data protection and AI

Personal data protection and AI

The Indonesian personal data protection regulatory framework (including: (i) Law No. 27 of 2022 on

Personal Data Protection, as amended ("**PDP Law**"); and (ii) other sectoral regulations containing PDP-related provisions, e.g., Law No. 11 of 2008 on Electronic Information and Transaction, as amended ("**EIT Law**"), along with its implementing regulations) provides specific requirements when processing personal data.

This is especially relevant as the PDP Law and EIT Law both have extraterritorial reach, affecting both domestic and overseas personal data processing of Indonesian data subjects.

A common use of AI involves web scraping of publicly available data from websites (e.g., gathering data from websites for a specific query, analysing news articles, reviewing job listings, etc.). Typically, such process can include the collection of publicly available personal data. Such use of AI tools should ensure adherence to PDP Law principles when processing the personal data of Indonesian data subjects, including reliance on appropriate lawful grounds. Considering that consent is impractical as AI tools conduct processing near instantaneously, providers of AI tools must assess other lawful grounds (i.e., other legitimate interest) and conduct assessments to comply with specific obligations.

As a practical matter, providers of AI tools should consider ensuring that their privacy policies are sufficiently comprehensive to explain personal data processing activities that may be involved in the use of their tools, including processing data from users and third-party sources. The wide (and sometimes complex) use cases of AI tools make it challenging to ensure all the mandatory information elements are included in privacy policies in a way that can be generally understood by the public.

The processing of personal data by AI tools may also necessitate a prior data protection impact assessment, as such processing could be classified as high risk under the PDP Law.

Protection of non-personal data and information

To protect technology and data (particularly non-personal data), companies typically apply a combination of statutory protections and contractual mechanisms. This layered approach is particularly relevant for protecting AI algorithms, which as abstract methods or procedures cannot be protected under copyright but may be safeguarded through other means. Law No. 30 of 2000 on Trade Secrets, as amended ("**Trade Secrets Law**") may be utilised to protect confidential know-how, model weights, proprietary datasets, training methodologies and internal processes. However, the Trade Secrets Law requires companies to implement real and demonstrable confidentiality measures – these typically include access control, non-disclosure agreements and internal policies.

3. Antitrust/competition laws

The Indonesian competition law framework, established by Law No. 5 of 1999 on the Prohibition of Monopolistic Practices and Unfair Business Competition (as lastly amended, the "**Competition Law**"), is administered by the Commission for the Supervision of Business Competition (*Komisi Pengawas Persaingan Usaha*, "**KPPU**").

While the Competition Law appears strict on its face, it has yet to respond – through formal instrument – to the development of digital markets and AI. However, the KPPU has observed that there is a need for provisions to be applied towards digital market monopoly. One particular concern on the KPPU's radar is algorithmic collusion, whereby the use of algorithms – and by extension, AI tools – could potentially enable digital market players to engage in price fixing or other unfair business practices. Oversight of these practices has become one of the KPPU's priorities.

4. Board of directors/governance

4.1 General Company Law considerations

There has yet to be a specific guideline for the use of AI within the context of company governance in

Indonesia. However, the basic Indonesian corporate governance rules and principles would generally apply to the use of AI for company governance.

The principles of Indonesian corporate governance stem from Law No. 40 of 2007 on Limited Liability Companies (as amended, the "**Company Law**"). In company governance, the board of directors is responsible for the management of the company, which must be conducted responsibly and in good faith. In this regard, the members of the board of directors can be held personally responsible for the losses of the company should they be at fault or negligently discharge their duties. Members of the board of directors can only be held exempt from such responsibility if they can prove lack of causation, good faith and duty of care have been fulfilled, no conflict of interest is present, and best efforts have been conducted to prevent losses.

Based on this understanding, the board of directors must ensure that any use of AI must not lessen their fiduciary duty for responsible management of the company. While AI may generally be used for routine and assistive tasks, overreliance on AI-driven decision-making could potentially give rise to claims of negligence or allegations that the board of directors failed to exercise appropriate duty of care. If such claims arise, shareholders have the right to file a lawsuit against the board of directors.

4.2 Other AI-specific guidelines considerations

Besides general governance principles stemming from the Company Law, several AI-related guidelines offer considerations on how company governance may be adapted in light of the use and development of AI. For instance:

- The OJK Code of Ethics (as defined and further discussed in section 5 "Regulations/government intervention" below) addresses the fair and accountable use of AI in the fintech industry, suggesting this may be supported by ensuring that AI-based business models do not adversely affect consumers or infringe upon their privacy. It also addresses transparent and explicable use of AI, suggesting that fintech companies maintain appropriate knowledge and control over their AI tools. These principles may serve as reference points when developing internal company guidelines.
- The AI Ethics Circular Letter (as defined and further discussed in section 5 "Regulations/government intervention" below) addresses the ethical use of AI through the lens of sustainable development, contemplating the potential impact of AI on humanity, the environment, and other living things. This perspective may offer an additional dimension for companies to consider when developing their environmental, social, and governance frameworks.

4.3 Data Protection Officer considerations

In terms of personal data protection-related governance, organisations utilising AI and Data-Driven Technologies may meet the criteria requiring appointment of a Data Protection Officer – particularly where such uses form part of the core activities involving periodical and systematic supervision of large-scale personal data.

5. Regulations/government intervention

Indonesia has yet to enact a dedicated regulation that governs AI. Currently, the Indonesian government is preparing a presidential regulation to establish a national AI roadmap and guidelines on the security of AI use (the AI Presidential Regulation). Each relevant ministry within the Indonesian government is expected to issue implementing regulations for each respective sector, including the MOCD.

Draft AI Presidential Regulation

At the time of writing this chapter, a publicly available draft of the AI Presidential Regulation has been circulated. In general, the draft AI Presidential Regulation reaffirms existing ethical values for the

development of AI, which has previously been adopted in a circular letter from the MOCD (as discussed below).

The draft AI Presidential Regulation envisages the following in terms of the AI ecosystem in Indonesia:

- AI is defined as technology that focuses on the development of a smart system, with explicit or implicit purpose, which is able to, autonomously or semi-autonomously, process data and information based on a variety of received inputs to produce outputs in the form of predictions, recommendations, content, or other decisions that impact the physical or digital environment.
- Stakeholders within the AI ecosystem in Indonesia consist of users, sector players, ministries/agencies, and other stakeholders (industry/business associations or parent companies).

Importantly, the draft AI Presidential Regulation seems to adopt a risk-based approach on the development and use of AI, classifying it into three categories: low risk; high risk; and unacceptable risk. The risk categories are defined as follows: unacceptable risk being that the use of such AI endangers the safety of the user; high risk being the use of such AI involving the use of specific personal data (as categorised under the PDP Law) and causing significant impact; and low risk being that the use of such AI has little to no threat to safety. These risks are assessed based on the macro and micro impacts of the AI use. Provided examples of micro risk factors include algorithm bias, disinformation, personal data violation, copyright violation, risks to vulnerable groups, etc. Provided examples of macro risk factors include impact of AI on strategic factors and fulfilment of public services functions.

The draft AI Presidential Regulation also requires users, sector players and authorities to implement risk mitigation measures in the development and use of AI. These risk mitigation measures are organised across several categories, including: protection of persons, the environment, and the state; mitigation of losses and misuse; transparency and accountability; fairness and adequacy; inclusivity and diversity; security through system reliability and technical expertise; consideration of arts and culture; and human oversight and control.

While there has yet to be a dedicated authority that will govern and supervise AI, the draft AI Presidential Regulation contemplates such role to be taken by the MOCD. It provides that the authority will monitor and evaluate AI and allow the reporting of AI ethics violations by users. The draft AI Presidential Regulation also establishes the National AI Ethics Forum to coordinate best practices in implementing AI ethics.

EIT Law

Under the EIT Law, AI should fall under the classification of "electronic agent". An electronic agent is defined as "*an electronic system that is made to automatically perform actions on certain electronic information that is managed/operated by persons*". This definition clearly captures the ability of AI to perform autonomously and interact with cyberspace, while still under the management/operation of a human operator (its user).

The EIT Law allocates the responsibility for an electronic transaction conducted through an electronic agent to rest in the organisers of the electronic agent. This is also applicable for failure of the electronic agent caused by actions of a third party. As a practical matter, providers of AI tools should consider establishing robust terms and conditions to facilitate appropriate allocation of liability and provide adequate disclosure regarding proper use of their AI tools.

In addition to its classification of an AI electronic agent, the EIT Law also classifies providers of AI tools as electronic service operators ("**ESOs**"). It must be noted that the EIT Law has extraterritorial scope as it applies to any overseas ESO as long as its system has a legal effect in Indonesian jurisdictions. Therefore, an overseas provider of AI tools is subject to the EIT Law if their AI tools can be utilised within Indonesia jurisdictions. Under the EIT Law and its implementing regulations, there are various compliance

requirements applicable for ESOs, which include mandatory ESO registration, ensuring the electronic system is safe and reliable, and ensuring no unlawful materials are produced on its electronic platform.

*MOCD Circular Letter No. 9 of 2023 on Artificial Intelligence Ethics ("**AI Ethics Circular Letter**")*

Issued in late 2023, the AI Ethics Circular Letter remains the sole officially issued ministerial guideline dedicated to regulating AI. Although the nature of circular letters is non-binding or high level, the AI Ethics Circular Letter provides the basis for the future of AI development and is thought to provide a glimpse into how AI will be regulated in Indonesia.

The AI Ethics Circular Letter provides that the development of AI must ensure the implementation of several values:

a. inclusivity, meaning the use of AI must result in information and innovation that reflect equality, fairness and peace;

b. humanity, meaning the use of AI must ensure the protection of human rights, social relations, beliefs and opinion of all peoples;

c. safety, meaning the use of AI must ensure the safety of its users and their data by protecting privacy and personal data, and prioritise their rights;

d. accessibility, meaning the use of AI must not be discriminatory as all users must have the same rights to access AI technology;

e. transparency, meaning the operation of AI must ensure transparency in the use of data for developing and operating AI systems;

f. credibility and accountability, meaning providers of AI systems must be able to take a decision over information and innovation resulting from AI and be held accountable for the actions resulting from their AI;

g. personal data protection, meaning the use of AI systems must ensure adherence to principles of personal data protection;

h. sustainability, meaning the use of AI systems must consider their impact on humanity and the environment to ensure sustainability and welfare; and

i. IP, whereby the use of AI systems must ensure the protection of IP.

Furthermore, it provides restriction on the use of AI, which must not concern policies or decisions that entail humanity. It also requires the prevention of racism and other acts that can damage humanity.

*OJK Code of Ethics Guidelines on Responsible and Trusted AI in Financial Technology Industry ("**OJK Code of Ethics**")*

Around the same time as the AI Ethics Circular Letter was issued, OJK, alongside several fintech business organisations, issued the OJK Code of Ethics, which outlines the basic principles for the use of AI in the fintech industry. It provides five principles:

a. Pancasila-based, meaning the use of AI by fintech in its business operation must be in line with Indonesia's official Pancasila ideology.

b. Beneficial, meaning that the fintech industry must ensure that the use of AI provides added value for business operations, which should increase the general welfare of consumers.

c. Fair and accountable, meaning that the use of AI must not cause losses, as well as ensuring the implementation of risk mitigation, the responsible use of datasets for training, and a high standard of testing.

d. Transparent and explicable, meaning that the fintech industry must ensure that it can explain how AI works and its application to the consumer so that the consumer can be adequately informed on the impact of the use of AI.

e. Robustness and security, meaning that the application of AI must go hand in hand with adequate cybersecurity measures to minimise security risks.

*Indonesia Press Council Regulation No. 1/Peraturan-DP/2025 on Guidelines for the Use of AI in Journalistic Works ("**Journalistic AI Regulation**")*

The Journalistic AI Regulation provides rules on how AI can be used in journalistic works in Indonesia. It provides that as a basic principle, the use of AI within journalistic works must be fully under the control of persons, be carried out in a responsible manner, and must be disclosed. It also provides that for the use of AI that produces the likeness of a person, prior consent must be obtained from all of the parties involved.

PR 32/2024

Relevant for the impact of AI to journalistic works, PR 32/2024 also contains provisions that can be relevant for AI tools providers, especially on the requirement to reduce bias. Providers of AI tools that can conduct web searches and collect information from online are required to provide their best effort to help commercialise news in Indonesia. It is also a requirement to provide "fair treatment" to all journalistic companies (i.e., publishers). Algorithms used by AI and Data-Driven Technologies must also be designed (using the best-effort basis) to distribute news that can reflect good-quality journalism and the values of democracy, diversity and the rule of law.

6. AI in the workplace

The adoption of AI and automation in Indonesian workplaces is considered essential as the government has identified digital transformation a key driver of economic growth.[1] Despite this, current Indonesian manpower regulation has yet to specifically address or consider the use of AI and its impact on manpower relations.

Generally, employers have wide discretion when hiring personnel and conducting performance evaluations. This includes the use of AI in human resources for assisting such functions. However, Law No. 13 of 2003 on Manpower (as amended, the "**Manpower Law**") prohibits discrimination that prevents the opportunity for work based on gender, race, ethnicity, religion and political beliefs. Accordingly, additional safeguards should be considered to help ensure that AI tools do not produce bias based on these factors when used in human resource functions.

While the benefits of AI and automation may cause companies to reduce their workforce to save costs and increase efficiency, the Manpower Law provides strict rules on employee terminations. As a basic principle, the Manpower Law requires employers to make an effort to avoid employee termination, which can only be engaged if it cannot be avoided. Termination cannot be carried out without cause and must be conducted based on one of the 14 officially recognised grounds for termination. While one of the recognised grounds for termination is for efficiency to prevent losses, in practice, such ground is subject to strict assessment and employers must be able to provide definite supporting proof of its claims. The Manpower Law also provides mandatory compensation requirements for terminated employees, which covers termination payment, long-service pay and compensation of rights. Should employees dispute their termination, they have the right to engage the employer in the industrial dispute resolution mechanism, which is often costly and prolonged.

Therefore, a careful assessment is advisable before employers consider reducing their workforce in favour of AI and automation, to evaluate whether the potential benefits outweigh the risks associated with employment-termination disputes.

7. Implementation of AI/big data/machine learning into businesses

In general, Indonesia has taken the approach of trying to balance support and facilitation of AI and Data-Driven Technologies' adoption by businesses in Indonesia, and compliance requirements aimed at protecting the interests of consumers and the general public.

When a business intends to launch or implement AI and Data-Driven Technologies in Indonesia, several key legal issues must be kept in mind:

- Registration-related compliance, especially if the AI is in the form of a user-facing platform – such user-facing platform would be subject to the registration requirement of the MOCD. This requirement extends to overseas platforms that are accessible in Indonesia. Failure to do so risks access blocking in Indonesia.
- Cybersecurity-related compliance – the EIT Law and regulations issued by the National Cyber and Crypto Agency contain security and reliability requirements applicable for electronic systems. This includes the requirement to implement SNI ISO/IEC 27001 and ensuring risk-management measures to ensure electronic system reliability, continuity of service and the protection of data.
- Unlawful content-related compliance – the EIT Law requirement for electronic system operators to ensure their platform does not contain unlawful content (pornography, online gambling, trade of unlawful substances, etc.) would be applicable. This requirement for platforms containing user-generated content (i.e., generative AI) is limited to taking down such unlawful content when its presence is detected/notified.
- Personal data protection-related compliance – should the AI and Data-Driven Technology involve the processing of personal data, businesses need to ensure that such processing complies with applicable personal data protection requirements, such as having an appropriate lawful ground, facilitating data subject rights, conducting recording of personal data processing activities, cross-border data transfer requirements, etc.

8. Civil liability

The civil liability concept for AI in Indonesia remains in its nascent stages, with courts and legal practitioners yet to issue any specific position or precedents on how existing legal frameworks apply to risk and liability issues for the use of AI systems. Instead, liability is constructed through general principles of civil law, primarily the Indonesian Civil Code, supplemented by sectoral regulations such as the Consumer Protection Law, PDP Law and EIT Law, as amended.

Under the Indonesian Civil Code, a party may claim civil liability that arises from losses resulting from another party's unlawful act. Generally, such claims require the establishment of causation, fault and the resulting damages in accordance with traditional legal standards. In the AI context, liability is not attributed to the system itself, as AI is not recognised as a legal subject under Indonesian law, but to the human or corporate actors who design, develop, deploy and control it. The legal focus therefore shifts from the autonomous output of the technology to whether those actors exercised reasonable care throughout the AI lifecycle. The broad understanding of unlawful act under Indonesian law typically encompasses violations of statutory provisions, rights, contractual obligations or duty of care. Any civil liability claims arising from AI-related harms would generally need to satisfy these requirements.

Sectoral regulations may also come into play for different types of harms caused by AI:

- Liabilities and responsibilities under the EIT Law – as operators of electronic agents, providers of AI tools/products would generally be liable for failure of the operation of the AI product, unless exemptions apply. Further, if illegal content (e.g., copyright infringement) is found in an electronic system (i.e., AI product/tool), in addition to potential liability over copyright infringement, the

access to the electronic system will be subject to access blocking by the MOCD – making the AI product/tool operator responsible for ensuring that their system does not include copyright-violating material.

- Liabilities for personal data protection – if the role of the providers of AI and Data-Driven Technologies is positioned as the personal data controller, it has the liability to compensate data subjects for failure of personal data protection.
- Draft AI Presidential Regulation – the responsibility to conduct risk management and risk mitigation on each lifecycle of an AI product is the responsibility of industry players. Based on this principle, the direction of liability for AI-related adverse effects appears to be shifting towards industry players; however, such liability may potentially be mitigated where best efforts in risk mitigation and risk management have been implemented.
- OJK Code of Ethics – the principle of fairness and accountability puts the burden on the financial service organiser to create an accountability framework for the output produced by an AI-based application. Such framework must be able to provide certainty for consumers in case of detrimental issues.
- Consumer protection – AI-generated products may also engage Indonesia's Consumer Protection Law, particularly around accuracy of information, safety, standard terms and fair business practices, with outcomes depending on how the AI is presented and used in context. In regulated finance, Bank Indonesia and the OJK consumer-protection and market-conduct requirements could extend to AI-mediated interactions, automated decisions, disclosures, complaint handling and safeguarding of customer data, though the precise implications will vary by use case and supervisory approach. The issued OJK Code of Ethics and AI Ethics Circular Letter place the protection of users and the public at the forefront – emphasising benefit, safety, fairness, transparency, accountability, and meaningful human oversight – which may indicate regulatory expectations for governance and risk controls without, by themselves, determining liability.

Endnote

1 https://ps-engage.com/indonesias-ai-national-roadmap-white-paper-paving-the-way-toward-a-smarter-and-sovereign-digital-future

Abadi Abi Tisnadisastra

Tel: +62 21 3021 2222 / Email: abadi.t@morihamada.com

Abi's practice covers a broad range of corporate and commercial areas, including M&A, restructuring, joint ventures and foreign investment. He has been involved in numerous cross-border acquisitions and investments in companies from various industries, including banking, financial services, manufacturing, information technology, e-commerce and financial technology (Fintech). He also advises foreign investors on operations, corporate governance, and legal compliance, whether at the outset of their investment or in connection with the compliant functioning of their ongoing businesses.

Abi is recognised for his in-depth knowledge of the financial services and information technology sectors, having advised local and multinational financial institutions (multi-finance, insurance, and venture capital companies), tech players, and investors in investing and consolidating operations in Indonesia. He advises clients across the Fintech ecosystem from start-ups to large technology companies, tech investors and financial institutions, as well as industry associations. Abi also counsels clients on data protection and privacy, blockchain technology and cryptocurrency.

Prayoga Mokoginta

Tel: +62 21 3021 2222 / Email: prayoga.m@morihamada.com

Yoga specialises in advising on tech-related legal matters. While he handles a variety of areas of legal practice, Yoga mainly focuses his practice on representing Indonesian and multinational clients in M&A transactions, personal data protection/data privacy, technology, fintech and payment system, e-commerce and general corporate legal matters.

He has an in-depth understanding of regulatory frameworks as well as extensive industry best-practice knowledge in the field of personal data protection and the tech industry. Yoga has also authored multiple international publications on such topics, notably, the 2024 and 2025 editions of *International Comparative Legal Guide – Data Protection*, as well as *Lexology – Due Diligence for Tech M&A in Indonesia 2024*.

Aloysius Andrew Jonathan

Tel: +62 21 3021 2222 / Email: andrew.j@morihamada.com

Andrew specialises in personal data protection/data privacy compliance, fintech, payment services, e-commerce regulations, and other tech-related legal matters. Andrew also has experience in advising clients on employment, anti-bribery/corruption, and general corporate compliance issues, as well as assisting multinational clients in conducting internal investigations and cross-border M&A.

Prior to joining ATD Law, Andrew previously assisted, as an intern, one of the reputable law firms in Indonesia that specialises in dispute and arbitration matters. Andrew holds a Bachelor's degree in law (S.H.) from Universitas Prasetiya Mulya.

ATD Law in association with Mori Hamada

Sequis Tower, 10th Floor, SCBD, Jl. Jend. Sudirman No. 71, South Jakarta, DKI Jakarta 12190, Indonesia
Tel: +62 21 3021 2222 / URL: www.atdmorihamada.com

Global Legal Insights – AI, Machine Learning & Big Data provides analysis, insight and intelligence across 22 jurisdictions, covering:

- Trends
- Ownership/protection
- Antitrust/competition laws
- Board of directors/governance
- Regulations/government intervention
- Generative AI/foundation models
- AI in the workplace
- Implementation of AI/big data/machine learning into businesses
- Civil liability
- Criminal issues
- Discrimination and bias
- National security and military

globallegalinsights.com