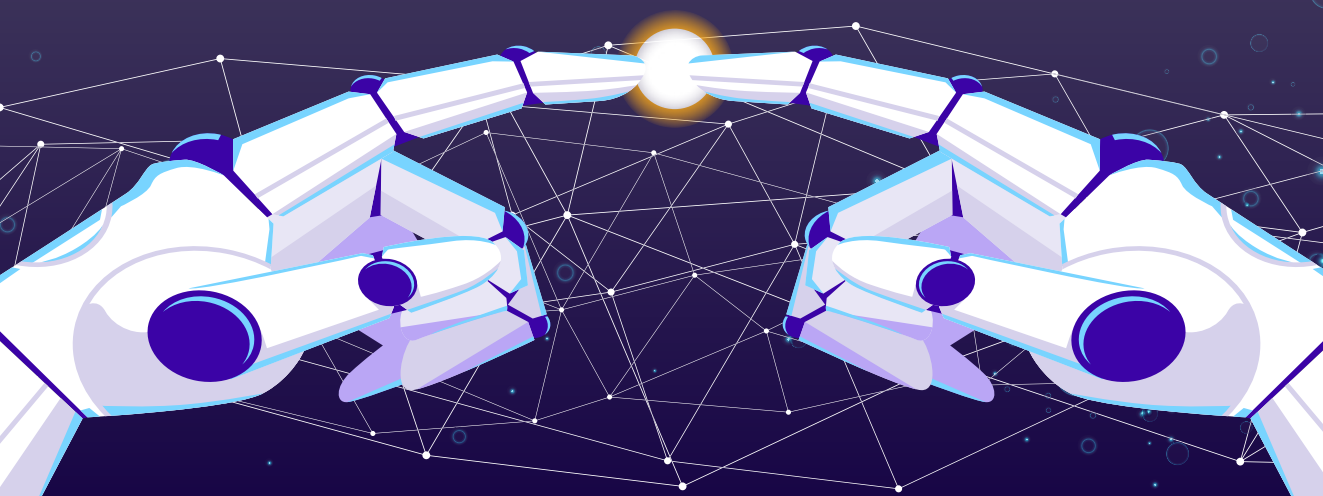
ACTIO

ISSUE #16 / AGUSTUS 2021

2020 Draft Bill on Personal Data Protection: Next Step of MoCI Regulation 20/2016

Digital Footprints Protection Under Indonesian Law

Legal Protection for the Community Against Misuse of Personal Data



KEY LEGAL ISSUES AND RISK OF COMPLIANCE IN DIGITAL TRANSFORMATION

9 772528 280004

INDONESIAN E-MAGAZINE FOR LEGAL KNOWLEDGE BY ANGGRAENI and Partners

ADVERTISING

AKASA CIPTA TAMA

We, Akasa Cipta Tama (ACT), was established in April 2015 as a response to the demand of highly qualified translators for business, legal, technical, and general documents; as well as interpreters and note takers for meetings, seminars, and conference. Our translators, interpreters and note takers have extensive experiences in their respective fields.

With a comprehensive database of qualified human resources, ACT works to ensure the best results in every project we run. Some of our top personnel have worked for various international events and some of our clients include the Office of the President of the Republic of Indonesia, People's Consultative Assembly, The United Nations, The World Bank, AusAID, USAID, and some prominent law firms in Indonesia.

Please do not hesitate to contact us if you have any question at marketing.akasa@gmail.com.
Looking forward to hearing from you.

CONTENTS

FOREWORD 3

INFO: Transformation of OSS (Online Single Submission) System in Indonesia 4

Q N A 5

OPINION: Digital Footprints Protection Under Indonesian Law 7

IN-DEPTH LOOK: 2020 Draft Bill on Personal Data Protection: Next Step of MoCI Regulation 20/2016 9

ANALYSIS: Legal Protection for the Community Against Misuse of Personal Data 11

LAW LAB: Beyond the Regulations: Artificial Intelligence in the Field of Contract Law 13

TIPS: Whistleblowing Procedures in The Environment of State-Owned Enterprise 15

ACTIO

Editorial:
Supervisor:
Setyawati Fitri A., S.H., LL.M., FCIArb., FAIADR.

Editor-in-Chief:
Sechabudin, S.H.
M. Adhima Djawahir, S.H.

Writers:
Dr. Hary Elias, BA V (Cantab), LL.M (1st Class Hons), MBA (Columbia), Juris Doctor (HES)
Tanya Widjaja Kusumah, S.H. (TWK)
Hendrikus Andy Leon Theovanus, S.H. (HAL)
Agustin L.H. Hutabarat, S.H., C.L.A. (ALH)
Yoga Adi Nugraha, S.H. (YAN)
Mochammad Adhima Djawahir, S.H. (MAD)
Sheila Putri Alina, S.H. (SPA)
Diara Rizqika Putri, S.H. (DRP)
Sechabudin, S.H. (SCN)
Febriana Dwi Hapsari, S.H. (FDH)
Keshia Bucha, S.H (KBA)
Frans Manuel Pakpahan,S.H. (FMP)
Sri Purnama, S.H. (SPU)
Media Consultant:
Fifi Juliana Jelita
Script Editor:
Wahyu Hardjanto
Visual Stylist:
Riesma Pawestri
Illustration: **freepik.com**
Actio Magazine is published every four months, made and distributed by:

ANGGRAENI and Partners

"Every industry and every organization will have to transform itself in the next few years. What is coming at us is bigger than the original internet, and you need to understand it, get on board with it, and figure out how to transform your business".

- Tim O'Reilly - Founder & CEO of O'Reilly Media -

Dear Reader,

Warm greetings to all readers. We hope that everyone is safe, healthy, and happy.

ACTIO is here again for readers with the main theme for this edition "Key Legal Issues and Risk of Compliance in Digital Transformation".

The Covid -19 Pandemic is still continuing and is currently entering its second year since the pandemic began at the end of 2019. During the current pandemic the government, private companies and other individuals and businesses are being conducted online, forcing all of us to embrace this digital transformation. However, there are many key legal issues and risks of compliance related to the growth, development and digital transformation in the business world.

ACTIO #16 discusses Key Legal Issues and Risk of Compliance in Digital Transformation, including: Procedures for reporting whistle blowing in State-Owned Enterprises, the OSS system transformation in Indonesia, data and information and its new criminal sanctions, implementation of good corporate governance, RUU 2020 about personal data protection that was not regulated in the Perkominfo 20/2016, and the protection of digital footprints.

We hope that this edition will provide useful information for all readers as we continue our digital journey together.

Happy Reading

ANGGRAENI AND PARTNERS

Setyawati Fitri A, S.H., LL.M., FCIArb
Partner Pengelola

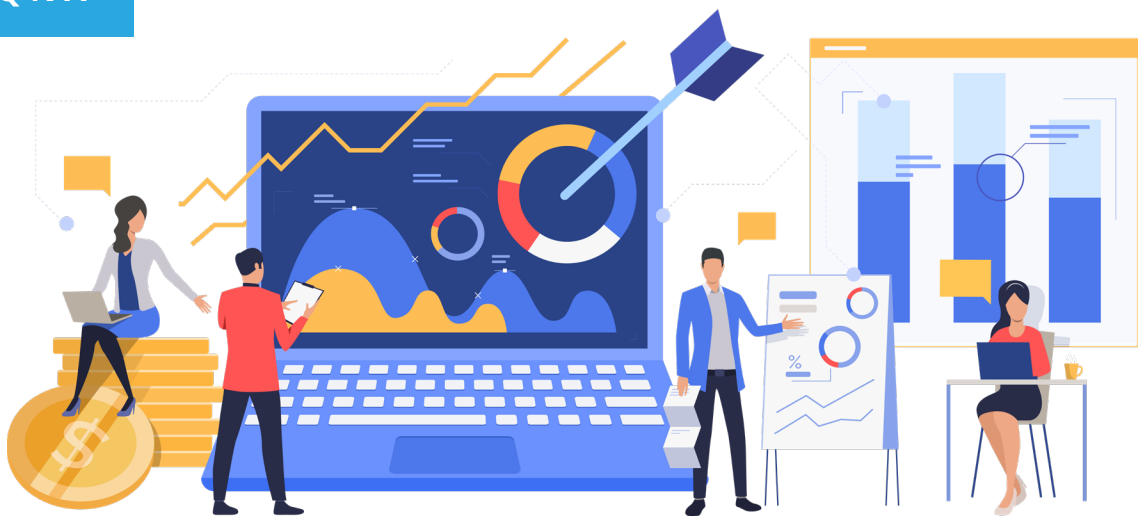
TRANSFORMATION OF OSS (ONLINE SINGLE SUBMISSION) SYSTEM IN INDONESIA

Compliance of a registered company in Indonesia is closely related to business licensing. One of the important aspects that support the business licensing system in Indonesia is the existence of the Online Single Submission (OSS) system. After the enactment of Law Number 11 of 2020 on Job Creation (Omnibus Law) and Government Regulation Number 5 of 2021 on Implementation of Risk-Based Business Licensing (GR 5/2021), a new concept of business licensing in Indonesia is recognized, namely Risk-Based Business Licensing, where the business license which is required by to the business actor is assessed based on the level of risk of the business activities concerned.

Prior to the enactment of the Omnibus Law, the business licensing approach in Indonesia was still in the form of a license approach, where supervision was more focused on fulfilling administrative requirements in obtaining a license. After the enactment of the Omnibus Law, the licensing approach is now shifting towards a risk-based approach. In Risk-Based Business Licensing, supervision is more focused on the implementation of the business activity to meet the standards and requirements of such a business activity.[1]

As a follow-up to the enactment of GR 5/2021, from 2 June 2021 to 1 July 2021, the government has conducted the trial implementation of the new OSS system that is oriented to risk-based business licensing, known as OSS-RBA (risk based approaches).[2] Risk-Based Business Licensing through the OSS System began implementation on 2 July 2021.[3] As for the fulfillment of commitments and applications for new business licenses by business actors submitted to the OSS system after 25 June 2021 where business licenses (effective business licenses) has not been issued by OSS system until 30 June 2021, the business licenses will then be processed based on Risk-Based Business Licensing in accordance with the provisions stipulated in GR 5/2021.[4] **ALH/HAL**

1. https://www.kominfo.go.id/content/detail/31693/uu-cipta-kerja-beri-kepastian-dan-penegakan-hukum-dalam-proses-perizinan-berusaha/0/berita, accessed on 15 July 2021
2. https://oss.go.id/portal/informasi/content/dtl_pengumuman/36 , accessed on 13 July 2021
3. Minister of Investment/Head of Indonesia Investment Coordinating Board Circular Letter Number 14 of 2021 on Transition of Implementation of Business Licensing to Implementation of Risk-Based Business Licensing Through OSS System
4. *ibid.*



What is Corporate Governance?

There is no one definition that is generally accepted and applied to every situation or jurisdiction. However, The Indonesia Corporate Governance Manual published by Indonesia's Financial Services Authority or Otoritas Jasa Keuangan (OJK) and the International Financial Corporation (IFC) provides a definition of Corporate Governance (CG) as structures and processes for the direction and control of companies.[1] There are four main principles to establish Good Corporate Governance (GCG) according to the OECD Principles, namely: fairness and equality, responsibility, transparency, and accountability.[2] There is one more principle that is deemed necessary to achieve GCG, namely independence. This GCG principle is needed to achieve the company's business sustainability in regard to minority shareholders and other stakeholders.

What are the laws and regulations governing Good Corporate Governance?

Law Number 40 of 2007 concerning Limited Liability Companies (Company Law) does not explicitly regulate GCG but provides important points in the implementation of GCG in companies.[3] The GCG terminology can be found in the Financial Services Authority Regulations or Peraturan Otoritas Jasa Keuangan (POJK), such as POJK 73/2016 concerning Good Corporate Governance for Insurance Companies and POJK 29/2020 concerning Amendments to POJK 30/2014 concerning Good Corporate Governance for Financing Companies.[4] This is because OJK as an independent institution, has the function of implementing an integrated regulatory and supervisory system for all activities in the financial services sector,[5] which tends to

1. International Financial Corporation (IFC) is a subsidiary company of the World Bank. IFC, The Indonesia Corporate Governance Manual: First Edition", (Jakarta: IFC, 2014), pp. 30.
2. OECD Principles created in 1999 and revised in 2004. It is accessible through: https://oecd.org/.
3. These regulations can be found in:
   i. Transparency is regulated in, amongst others, Article 8 paragraph (2) letter b; Article 29 paragraph (5); Article 66 paragraph (1) dan (2); Article 67 paragraph (1); Article 69 paragraph (3); Article 100 paragraph (1) letter b; Article 68 paragraph (1); Article 75 paragraph (2) Company Law.
   ii. Accountability is regulated in, amongst others, Article 12; Article 13; Article 14; Article 49 paragraph (2); Article 50; Article 56; Article 100 paragraph (1) letter a; Article 63; Article 64; Article 92 paragraph (1); Article 97 paragraph (1); Article 97 paragraph (2); Article 97 paragraph (3); Article 108 paragraph (1); Article 144 paragraph (1); Article 114 paragraph (2) Company Law.
   iii. Responsibility is regulated in, amongst others, Article 24; Article 25; Article 74; Article 138 paragraph (1) Company Law.
   iv. Independency is regulated in, amongst others, Article 36 paragraph (1); Article 85 paragraph (4); Article 97 paragraph (5) letter c; Article 99 paragraph (1) letter b; Article 101 paragraph (1) Company Law.
   v. Fairness and equality is regulated in, amongst others, Article 3 paragraph (1); Article 3 paragraph (2); Article 51; Article 52 paragraph (1); Article 66 paragraph (1); Article 66 paragraph (2); Article 102 paragraph (1); Article 89 paragraph (1); Article 53 paragraph (2); Article 82 paragraph (4); Article 84 paragraph (1); Article 85 paragraph (1); Article 61 paragraph (1); Article 61 paragraph (2); Article 62 paragraph (1); Article 62 paragraph (2); Article 43 paragraph (1); Article 97 paragraph (6); Article 114 paragraph (6); dan Article 138 paragraph (3) Company Law.
4. Other regulations issued by OJK that regulate Governance can be found in, amongst others, POJK 55/2016 concerning Implementation of Governance for Commercial Banks; POJK 21/2015 concerning Implementation of Public Company Governance Guidelines; POJK 29/2020 concerning Amendments to POJK 30/2014 concerning Good Corporate Governance for Financing Companies.
5. Article 5, Law Number 21 of 2011 concerning Financial Services Authority.

require higher legal compliance. Thus, regulations regarding good GCG standards must be formulated for company activities related to financial services. In addition, CG can also be found in the Decree of the Minister of SOEs KEP-117/M-MBU/2002 concerning the Implementation of GCG Practices in State-Owned Enterprises or Badan Usaha Milik Negara (BUMN) providing a definition of CG, namely, as a process and structure used by BUMN organs to improve business success and corporate accountability in order to realise shareholder value in the long term while taking into account the interests of other stakeholders, based on laws and regulations and ethical values.[6]

How important is it to implement Good Corporate Governance?

The implementation of GCG in the company is very important so that the company's goals are achieved without harming any party and stakeholder. Democratic priciples of one share, one vote, may be open to abuse, usually to the detriment of the minority shareholder. Access to decision making to Board Level and Senior Management positions are also often less transparent and Executive and Director Remuneration are open to abuse. The implementation of GCG has a positive impact on the company by increasing the value of the company. This is because the principles of GCG promote transparency, especially on crucial matters, such as the company's financial statements, competence of Board of Directors, optimising decision making, and increasing employee motivation. Problems such as abuse of authority that harm the company can be minimised by implementing GCG. GCG promotes investors' and the public perception that the company has its commercial interests at heart when making decisions. This increases confidence and the value of the company increases. In the long term, the implementation of GCG is also a guarantee for the creation of a good corporate culture that can continue to maintain a sustainable corporate reputation. In a broader perspective, GCG also encourages the creation of an efficient and consistent market that is economically beneficial for the country. **TWK/SPU**

6. Article 1 letter a, Decree of the Minister of SOEs KEP-117/M-MBU/2002 concerning the Implementation of Good Corporate Governance Practices in State-Owned Enterprises (Badan Usaha Milik Negara or BUMN).

DIGITAL FOOTPRINTS PROTECTION UNDER INDONESIAN LAW

Digital footprints or more commonly known as cookies on some sites, is a set of text that is stored on a person's computer or device by a website that is visited by that person.[1] A cookie can record information on sites that have been visited, items added to a digital shopping cart, or information that has been filled in into digital forms, such as names and passwords.[2] Cookies also has function so that the ads shown to users are relevant and not displayed repetitively.[3]

Digital footprints can be useful for making users surf the Internet easier. However, users have little control over who collects this information or where it is sent. By design, users can delete digital footprints from their own browsers, but users will not be able to manage or delete the digital footprints in the third party's servers that store and collect the data, for example the site administrator.[4] For example, the official website of Honda Indonesia informs that information regarding the digital footprint contained on that page will be shared with service providers, business transfers, affiliates, and business partners.[5] However, the users do not obtain information in detail concerning the identity of the parties who receive the relevant digital footprint.

Indonesian laws and regulations do not provide a specific definition of digital footprints. The regulation most closely related to the digital footprints is Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 19 of 2016 (Law 11/2008) and its implementing regulation namely Government Regulation Number 71 of 2019 concerning The Organization of Electronic Systems and Transactions (GR 71/2019), namely the provisions regarding personal data.

1. https://support.mozilla.org/id/kb/Tentang%20Cookie, accessed on 21 July 2021.
2. https://www.republika.co.id/berita/q45k7h370/kebijakan-privasi-baru-google-batasi-emweb-cookieem, accessed on 13 July 2021.
3. https://support.google.com/adsense/answer/7549925?hl=en, accessed on 5 July 2021.
4. https://tinuiti.com/blog/data-privacy/what-is-a-cookie-and-why-are-third-party-cookies-going-away/, accessed on 12 July 2021.
5. https://www.honda-indonesia.com/privacy-policy, accessed on 5 July 2021.

Pursuant to Article 1 number 29 GR 71/2019, Personal Data is any data on a person, which is identified and/or may be identified individually or combined with other information both directly and indirectly through an electronic system and/or non-electronic system. Based on this provision, GR 71/2019 provides a very broad definition of Personal Data, which at a glance, may be interpreted to include digital footprints as part of Personal Data.

However, this interpretation must also consider the concept of the digital footprints itself. A digital footprint is a collection of traces of all digital data, including any and all files and accounts, whether stored locally on a device or online,[6] originating from a device that is used to access the internet, regardless of who and how many people use the device, only 1 (one) profile will be formed after the digital footprint is processed. This is in principle different from personal data, which tends to be attached to a person.

Regardless of the difference, Law 11/2008 regulates that unless determined otherwise by laws and regulations, the use of any information through electronic media, which is related to Personal Data of a person shall be conducted with the consent from the person concerned.[7] GR 71/2019 also regulates that Electronic System Providers[8] must implement the principle of Personal Data protection in processing Personal Data, including but not limited to collection of Personal Data and must be conducted in a limited and specific manner, legally valid, fair, with the consent and agreement of the Personal Data owner.[9] Further, the Electronic System Provider must provide information to the user concerning a privacy and/or protection of Personal Data guarantee.[10]

The existing provisions seem to focus on notification and users' consent for the management of the digital data, but there is no clear provision regarding the prohibition on the collection of certain Personal Data and further, no provision regarding the monetization of digital footprints. By considering the very broad definition of Personal Data and also the current business developments, there will potentially vast amount of users' personal information that can be collected, monetized, and potentially misused.

Law 11/2008 has given rights for every person who considers his privacy rights are violated,[11] or suffer loss in relation of organizations of electronic system and/or uses information technology[12] to file a lawsuit. However, this provision will be very difficult to implement in practice because there is a tendency that users are not aware of what digital footprints are left, especially passive digital footprints, and by whom the digital footprints are used to cause loss.

In the end, a specific provision is needed in the laws and regulations regarding how to collect, process, limit, and prohibit the use of personal digital data in general and digital footprints in particular. It is not sufficient to only regulate the legal remedies in the event of misuse of digital footprints, but it is necessary to make a prohibition and provide preventive provision so that the protection of digital footprints and personal rights of each person can be safeguarded and its use carried out optimally for the stated purpose of allowing the user a better surfing experience online. **DRP/SCN**

6. Sandi S. Varnando, Your Digital Footprint Left Behind at Death: An Illustration of Technology Leaving the Law Behind, Vol. 74-No. 3 Spring 2014, page 721.
7. Article 26 paragraph (1) Law 11/2008.
8. According to Article 1 number 4 GR 71/2019, Electronic System Provider is any Person, state administrator, Business Entity, and the public which provides, manages, and/or operates Electronic System individually or jointly to Electronic System User for their own purposes and/or for other parties' purposes
9. Article 14 GR 71/2019.
10. Article 29 GR 71/2019.
11. Article 26 paragraph (2) Law 11/2008.
12. Article 38 paragraph (1) Law 11/2008.

2020 DRAFT BILL ON PERSONAL DATA PROTECTION: NEXT STEP OF MOCI REGULATION 20/2016

Personal Data Protection is an important issue in the digitalization era, and it is essential to regulate data protection under the law as a form of recognition and guarantee of the protection of the citizens' right to privacy. Personal Data Protection in Indonesia is currently regulated under the Minister of Communication and Informatics Regulation Number 20 of 2016 concerning Protection of Data Protection in Electronic Systems (MoCI Regulation 20/2016) and Government Regulation Number 71 of 2019 concerning Organization of Electronic Systems and Transactions (GR 71/2019).

However, to provide a legal framework that further guarantees the personal data protection, the Government has officially submitted the Protection Data Protection Final Draft Bill (PDP Draft Bill) on the 24 January 2020 to the House of Representatives through President Letter Number: R-05/Pres/01/2020.[1] The PDP Draft Bill provides legal certainty to guarantee and protect the rights of Personal Data Owners, such as:

(i) the right to request information regarding the underlying purpose for the acquisition and use of personal data;
(ii) the right to access their personal data;
(iii) the right to complete, update, or correct their personal data;
(iv) the right to terminate, delete, and/or eliminate their personal data;
(v) the right to revoke their consent for the use of their personal data;
(vi) the right to delay or limit the processing of their personal data; and
(vii) the right to file lawsuits and obtain compensation in relation to violations of personal data.[2]

1. https://kominfo.go.id/content/detail/24039/siaran-pers-no-15hmkominfo012020-tentang-presiden-serahkan-naskah-ruu-pdp-ke-dpr-ri/0/siaran_pers
2. RUU PDP, Pasal 4-14.

As a side note, there are some exceptions to the protection of these rights, for instance in the interest of national defense and security, the law enforcement process, public interest, supervision of the financial services sector, and official scientific research conducted by the state.[3]

To ensure that the rights of the Personal Data Owners as stated above can be protected, the PDP Draft Bill also stipulates that the Personal Data[4] Controller must maintain the confidentiality of the Personal Data and must obtain written or verbal approval beforehand from the Personal Data Owner through electronic or non-electronic means before they can carry out data processing.

In order to obtain such approval, the Personal Data Controller is required to provide information concerning the legality and purpose of data processing,[5] type and relevance of the personal data, a document retention period, details regarding the information collected, a processing period, and the rights of the Personal Data owner.[6] However, there are exceptions of such approval in certain circumstances as follows:

(i) fulfillment of the agreement in the event that the Personal Data Owner is a party or fulfillment of request from Personal Data Owner to comply with the agreement;
(ii) fulfilment of the Personal Data Controller's legal obligation in accordance with the laws and regulations;
(iii) fulfillment of Personal Data Owner's legitimate interests;
(iv) implementation of the Personal Data Controller's authority;
(v) fulfillment of the Personal Data Controller's obligations for the public service; and/or
(vi) fulfillment of other legitimate interests by taking into account the interests of the Personal Data Controller and Owner.[7]

Further, PDP Draft Bill also stipulates that Personal Data Controller and Personal Data Processors are required to appoint Personal Data Protection Officers[8] in certain cases, for example for the interest of public services, for the main activity of Personal Data Controller that requires regular and systematic monitoring of Personal Data on a large scale, and where the processing of Personal Data is for a specific and/or related to a criminal offence.[9] Personal Data Protection Officers have the duty to inform and provide advice to the Personal Data Controller or Personal Data Processor regarding the compliance with the PDP Draft Bill, to supervise the compliance with the PDP Draft Bill, and to cooperate with relevant parties concerning the personal data protection.[10]

The PDP Draft Bill also stipulates administrative sanctions for several offences through written notices, temporary termination of Personal Data processing activities, removal or elimination of Personal Data, compensation, and/or administrative fines.[11] In addition to administrative sanctions, there are also several violations that are subject to criminal sanctions or imprisonment, for instance collection of personal data that causes harm to the Personal Data Owner, unlawful disclosure and use of the Personal Data, forgery of Personal Data for commercial purposes, and unlawful trade of personal data.[12] **SPA/YAN**

3. RUU PDP, Pasal 16.
4. PDP Draft Bill, Article 21.
5. PDP Draft Bill, Article 19 paragraph (1) and (2).
6. PDP Draft Bill, Article 24 paragraph (1).
7. PDP Draft Bill, Article 18.
8. PDP Draft Bill, Article 45 paragraph (1).
9. PDP Draft Bill, Article 45 paragraph (2).
10. PDP Draft Bill, Article 46.
11. PDP Draft Bill, Article 51
12. PDP Draft Bill, Article 61-69.

LEGAL PROTECTION FOR THE COMMUNITY AGAINST MISUSE OF PERSONAL DATA

In the use of Information Technology, the protection of personal data is generally regarded as a part of privacy rights, which have the following meanings: (i) personal rights are the rights to enjoy a private life and be free from all kinds of interference; (ii) privacy rights are the rights to be able to communicate with other people without spying; (iii) privacy rights is the right to monitor access to information about a person's personal life and data.[1]

1. Elucidation of Article 26 paragraph (1) Article 26 paragraph 1 of Law Number 11 of 2008 which has been amended by Law Number 19 of 2016.

Personal information includes everything related to a person's personal data, for example biometric data such as height, weight, blood type, fingerprint, retina, DNA, or other health conditions, or immigration travel data, criminal history, education, bank accounts, telephone number, and other personal data attached to the individual. al. In essence, when the information is not tied to the individual who has the information, then the information can only be said to be not personal information.[2]

Along with the development of technology, the misuse and theft of personal data is a phenomenon that often occurs. One of the causes of the misuse and theft of personal data is our own negligence when dealing with our own information, especially in our daily activities whilst using the Internet.

Some examples that often occur are: (i) providing personal data to the seller when buying a SIM card; (ii) downloading unsafe applications; (iii) attaching personal data in platforms or other forms, which can be misused by various parties and potentially may cause harm to the data owner. Therefore, Article 26 paragraph 1 of Law Number 11 of 2008, as amended by Law Number 19 of 2016 (ITE Law), stipulates that the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned, unless stipulated differently by laws and regulations.

If this provision is violated, then everyone whose rights are violated have the right to file claims for compensation against the party who used personal data without consent.[3] Personal Protection is also regulated in the Regulation of the Minister of Information and Communication Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems (Permenkominfo 20/2016) which explains that data owners can submit complaints to the Ministry of Communication and Information for the failure to protect the confidentiality of personal data.[4]

The government can also impose administrative sanctions on any party who misuses personal data in the form of a:[5]
a. Verbal warning;
b. Written warning;
c. Temporary suspension of activities; and/or
d. Announcement of sites in the network (online website).

With the existence of a legal basis for sanctions and punishments against wrongdoers, the community, especially data owners, can now expect a sense of security and comfort for data owners. Hopefully, this legislation will deter the crimes of misuse and theft of personal data and information. **KBA/FDH**

2. Jerry Kang, "Information Privacy in Cyberspace Transactions", Stanford Law Review, Vol. 50, No. 1193, 1998, p. 1207-120.
3. Article 26 paragraph (1), ITE Law
4. Article 26 letter b, Permenkominfo 20/2016
5. Article 36 paragraph (1) letter a to d, Permenkominfo 20/2016

BEYOND THE REGULATIONS: ARTIFICIAL INTELLIGENCE IN THE FIELD OF CONTRACT LAW

Law is a tool that intersects in almost, if not, all aspects of life including education, social interaction, and businesses. In this era, where technological advancement is an inevitable event that society faces, questions arise as to what extent these changes affect the law or whether or not the law can catch up to regulate—what is known as the unregulated—Artificial Intelligence (AI).

Haenlein and Kaplan define AI as, "a system's ability to correctly interpret external data, to learn from such data, and to use those learnings to achieve specific goals and tasks through flexible adaption."[1] This means the abilities that AI are expected to have are similar to human capabilities, such as visual perception, speech recognition, decision-making, and translation between languages. For instance, self-driving cars and chatbots are powered by AI. In the field of law, AI usually comes in the form of contract drafting, contract review, contract analytics, litigation prediction, and legal research, which offers acceleration and efficiency in the legal industry.

This existence of AI in the field of law arises multiple questions we should all be asking. Can AI one day be expected to supervise and enforce the contract that it has written?

Up to this point, the AI system offers limited capabilities as mentioned above. Yet, this does not stop the possibility that one day, AI will have the ability to supervise and enforce a written contract. For example, the usage of AI in a transaction agreement. With the data that it has gathered, an AI software can easily detect which party failed to implement the agreement or even determine if the contracting Parties was performed dishonestly. Without errors, AI can also identify which clause

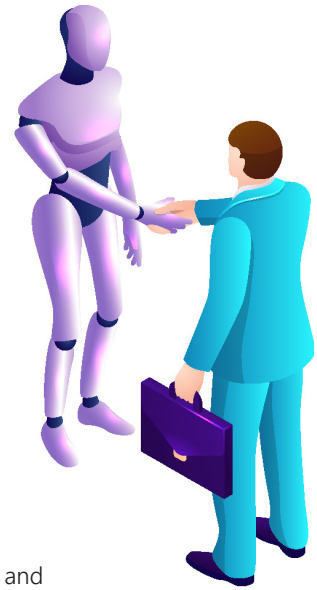
1. Michael Haenlein and Andreas Kaplan, "A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence", in California Management Review, (2019), pp. 1 in Christoph Bartneck, et. al., "What is AI?" in An Introduction to Ethics in Robotics and AI, (New York: Springer, 2021), pp. 5-16.

the party has breached and what punishments or compensations the party should bear due to that breach of contract. These are nit the fanciful musings with the exponential rate of development in AI.

One of the current leading AI systems is Kira Systems,[2] an AI software that claims to identify, extract, and analyse content in legal contracts and documents with unparalleled accuracy and efficacy. This system is currently being used by global law firms such as Hogan Lovells, Gorissen Federspiel, Osler, Shapman and Cutler LLP, Loyens and Loeff, Nagashima Ohno & Tsunematsu and many more.

Other honourable mentions of Legal AI start-ups are Leverton, ContractPod, ThoughtRiver, and so on.[3] With more Legal AI start-ups emerging and more law firms using AI in their legal practice, this leads to the next question: What are the moral boundaries when it comes to law enforcement by the AI?

Unlike the judges who listen to both parties before rendering a decision, AI could easily appears to remove the noise and clutter, rendering a decision based on real live data and while calculating risks. No 'good faith' is going to be considered nor the true intentions of such deeds. As Gustav Radbruch postulated that the idea of law is defined through a triad of justice, utility, and certainty,[4] can it be guaranteed the decisions that are based on data and AI's considerations alone, fulfil that idea of law?



Some jurisdictions have made efforts to create relevant framework to govern the unabated growth of AI, namely Singapore's PDPC that released its first edition of the Model AI Governance Framework in 2019 as updated in 2020.[5] Brazil and Scotland recently launched their AI strategies, and the EU where the European Commission published its draft regulation for AI. Yet, none of these initiatives have been promulgated into laws.[6] In 2019, there were 42 countries that supported OECD Principles on AI. These principles are not binding on member countries, but it gives the sense of urgency that all have the same vision and framework to contain the growth of AI and why AI should be overseen.

Whilst the debate is ongoing, the technology keeps on updating. More questions will emerge as long as developers keep pushing the limits of AI to satisfy the never-ending curiosity about just how far can AI really go? At the end of the day, when technological advances are unavoidable, AI will either integrate with the law or abolish the law altogether. **SPU**

2. Kira, "How it Works?", https://kirasystems.com/how-kira-works/.
3. Industrywired, "10 Legal AI Startups Transforming the Way Legal Industry Operates", https://industrywired.com/10-legal-ai-startups-transforming-the-way-legal-industry-operates/.
4. Gustav Radbruch, Main Features of Legal Philosophy, in Anton-Hermann Chroust, "The Philosophy of Law of Gustav Radbruch", in The Philosophical Review, Vol. 53, No. 1, (January 1944), pp. 23-45.
5. The guiding principles of the framework are: (i) decisions made by AI should be explainable, transparent, and fair; (ii) AI systems should be human-centric. See, PDPC, "Singapore's Approach to AI Governance", https://www.pdpc.gov.sg/Help-and-Resources/2020/01/Model-AI-Governance-Framework.
6. Several legislations related to AI issues are being drafted in the United States, such as Alabama with their bill on establishing the Alabama Council on Advanced Technology and Artificial Intelligence to review and advise the Governor, the Legislature, and other interested parties on the use and development of advanced technology and artificial intelligence. The United Kingdom has a guidance regarding Artificial Intelligence provided by the Department for Digital, Culture, Media and Sport, on data ethics and the Alan Turing Institute, on responsible design and implementation of AI systems. In China, the regulation of AI is governed mainly by the State Council of the PRC's July 8, 2017 "A Next Generation Artificial Intelligence Development Plan" (State Council Document No. 35).

WHISTLEBLOWING PROCEDURES IN THE ENVIRONMENT OF STATE-OWNED ENTERPRISE[1]

A Whistle blowing system according to Chapter IV(a) Regulation of the Minister of State-Owned Enterprises Number: Per-01/MBU/01/2015 concerning Guidelines for Handling Conflicts of Interest in the Ministry of State-Owned Enterprise (RMSOE 01/2015) is a report mechanism made by Employees of the Ministry of State Owned Enterprise or other parties (State-Owned Enterprise Employee, work partners and the community) who do not have direct involvement, who are aware of the existence of a potential of a Conflict of Interest in the Ministry of State-Owned Enterprise and where the handling of the report is kept confidential.

Stages of Reporting on Alleged Conflict of Interest requiring Whistle Blowing

Based on the provisions of Chapter III (A)1 of the Regulation of the Minister of State-Owned Enterprise Number: Per-13/MBU/10/2015 concerning Guidelines for the Management of the Reporting System for Alleged Violation within the Ministry of State-Owned Enterprise (RMSOE 13/2015) explains that the Stages of Management of the Alleged Violation Reporting System must at least include (a) criteria and data for reporting alleged violation, (b) time of the report violation, (c) anonymous reporting and (d) a report submission mechanism.

The Criteria and Data for Reports of Alleged Violations as referred to in point (a) above are reported violations, which are at least manifested in the form of corruption and conflicts of interest (such as receiving gratuities, abusing positions, outside employment and so on see Chapter II letter A SOE Ministerial Regulation 01/2015). Therefore, report of alleged violations must meet the following elements:

a. There is a suspected violation.
b. Place where the alleged violation occurs.
c. When did the alleged violation occur.
d. The identity of the alleged violator.
e. Method used to commit the alleged violation.

Moreover, the report of alleged violation must be accompanied by Sufficient Preliminary Evidence, at least in the form of relevant data or documents and/or relevant images or recordings. Further,

1. The information is not intended to provide a legal opinion or views of the Anggraeni and Partners law offices against a particular legal issue. Neither party may assume that he or she should act or cease or choose to act on a particular matter based on this information without seeking advice from professionals in accordance with the certain facts and certain circumstances it faces.

the mechanism for submitting a report is a set out. Reports can be made through the existing infrastructure such as telephone, SMS Central, a Website, an e-mail, facsimile, or Official Letter from the Ministry of State-Owned Enterprise addressed to the Inspector. In addition to the communication channels above, reporting of alleged violations can also be done by reporting through formal channels (through the direct superiors or persons with related functions).[2]

Upon creating a report of alleged violation, the next step is recording, reviewing, and in particular to identify the nature of the violation and to formulate a mechanism for handling these alleged violations. The mechanism must also include forwarding them to the relevant Board of Directors and Board of Commissioners/Supervisory Boards, and subsequent archiving.[3]

Once these initial steps have been completed, further handling of reports of alleged violations are described in Chapter III (B) of Ministerial Regulation 13/2015, namely to carry out investigative audits and audits with specific objectives. An investigative audit is intended if there is an alleged violation that indicates a criminal act of corruption, while an audit with a specific purpose is suitable if the alleged violation indicates a deviation that is detrimental to state finances, personnel irregularities, procurement of goods and services, or other violations that are not criminal acts of corruption.

The conclusion is, the enactment of Ministerial Regulation 01/2015 and Ministerial Regulation 13/2015, especially within the Ministry of State-Owned Enterprise, has provided a guarantee of confidentiality to every Whistle blower who makes reports regarding suspected violations in the Ministry of State-Owned Enterprise. In addition, the 2 (two) regulations clearly explain the steps that can be carried out for making or filing a report regarding the allegations. It clearly protects the identity of the whistle blower at the Ministry of State-Owned Enterprise. Setting up this clear mechanism will go a long way to promote transparency by our officials in SOEs. **MAD/FMP**

2. See point 1 and point 2 letter (d) regarding the Mechanism for Submission of Reports for Chapter III of Minister of SOEs Regulation 13/2015.
3. See point 2 to point 5 letter (A) Chapter III of SOE Ministerial Decree 13/2015.

www.ap-lawsolution.com

TENDEAN SQUARE KAV. 17-18
Jl. Wolter Monginsidi No. 122-124
Kebayoran Baru, South Jakarta
Indonesia – 12170

PHONE : +62-21-72787678, 72795001
FAX : +62-21-7234151
EMAIL : connect@ap-lawsolution.net