ZICO | law

ASEAN INSIDERS
by origin and passion

DATA LEAKS IN HEAVY CYBERATTACK SEASON: INCREASING CONCERNS OVER PERSONAL DATA PROTECTION IN INDONESIA

With the recent cyberattack and data leak incidents in Indonesia, concerns over personal data protection have grown given that most of these cases are unresolved and perpetrators go unpunished.

In this article, Jade Hwang, Andina Sitoresmi and Randyaz Iskandar of Roosdiono&partners (a member of ZICO Law) shares their insights on the legal and regulatory framework of data protection in Indonesia including the latest Personal Data Protection Bill.

FEBRUARY 2022

As if the cyberattacks on State Intelligence Agency's server were not worrying enough, the recent cyberattacks on the National Cyber and Encryption Agency/*Badan Siber dan Sandi Negara* ("**BSSN**") have added to the long list of incidents on Electronic Systems[1] operated by the Indonesian Government. A Brazilian hacker identified as SonIx[2] has defaced the website of the national malware centre, which is supposed to detect and prevent cyberattacks in Indonesia. Prior to the cyberattack on the BSSN's website, the database of the Indonesian Child Protection Commission's/*Komisi Perlindungan Anak Indonesia* ("**KPAI**") that contains information about the people who filed reports on alleged child abuse cases, bullying, kidnapping, violence against children and rape was also hacked by a hacker identified as C77.

In mid-July, 2021, vpnMentor researchers reported that the personal information of some 1.3 million users of the electronic Health Alert Card ("**e-HAC**") test-and-trace application was not protected as the public could freely access the e-HAC's data through a popular search engine Elasticsearch.[3] President Joko Widodo's Personal Data[4] was also leaked and the public can download his COVID-19 vaccine certificate by entering his national identification number on Peduli Lindungi application ("**Peduli Lindungi App**"). The application that has over 10 million users and provides health information, vaccination data as well as mobility tracking to assist the Government in gaining data about the spread of COVID-19 should not disclose or transfer any data to other public data controllers.

Cyberattacks also happen on private Electronic System Providers[5] in all sectors. A Fintech aggregator platform, namely, *cermati.com* reported data leaks experienced by its 3 million users, and the information was reportedly sold online for USD2,200. Two unicorn e-commerce platforms, *Bukalapak* and *Tokopedia* also reported data breaches where the data of their users were sold on the dark web.

NOTABLE CASES OF PERSONAL DATA LEAKAGE IN INDONESIA BETWEEN 2019 - 2021

MARCH 2019 — In March 2019, a Pakistani hacker, "Gnosticplayers" claimed to have hacked a database containing 13 million data belonging to Bukalapak users and sold it on the dark website.

MAY 2020 — In early May 2020, Tokopedia was hacked, and it affected the data of 91 million Tokopedia users and more than 70 million merchant data. The data was allegedly sold on the dark website.

MAY 2020 — An Israeli cybersecurity consultant, *Under the Breach*, revealed that the data of 2.3 million Indonesians belonging to the General Elections Commission was leaked and offered on a hacking forum. The data belongs to voters in 2013.

JULY 2020 — In early July 2020, Cyble Inc, a cybersecurity company from Atlanta, United States, found 896,170 data belonging to Kreditplus customers put up for sale on internet forums.

MAY 2021 — A RaidForums user named "Kotz" sold a database containing the personal information of some Indonesians. The data sold includes resident identity card numbers, salaries, phone numbers, addresses, and emails. Kotz claimed the data was obtained from the website of the Health Social Security Agency.

JULY 2021 — In July 2021, data allegedly belonging to 2 million BRI Life insurance customers was offered on a hacking forum by a user named "Reckt".

AUGUST 2021 — A research team from vpnMentor found that around 1.3 million data belonging to users of the Indonesian Electronic Health Alert Card ("**e-HAC**") application developed by the Ministry of Health ("**MoH**") were exposed on the internet.

OCTOBER 2021 — A RaidForums user "C77" offered data belonging to the National Commission For Child Protection. The database is compiled in a tabular form in ".csv" file format and contains the personal data, such as name, resident identity card number, nationality, phone number, and occupation.

Undoubtedly, no ESP would intentionally create a faulty security system to make it easily hacked by any irresponsible party. Nonetheless, considering the number of cyberattack cases that remain unsolved and the fact that investigation may be discontinued just by providing a statement and assurance that "our data is secure", why does an ESP always consider itself as a victim rather than the perpetrator? Are we, as users, and citizens of Indonesia, adequately protected? What has been done to prevent these leaks from happening in the first place? And when the leak happens, what will they do to take responsibility? So far, we have only been hearing excuses.

---

[1] According to Article 1 paragraph (5) of Law No. 11 of 2008 on Electronic Information and Transaction, as amended by Law No. 19 of 2016 ("**ITE Law**"), an Electronic System is a series of electronic devices and procedures that function to prepare, collect, process, analyse, store, display, announce, transmit, and/or disseminate electronic information ("**Electronic System**").

[2] On 19 November 2021, SonIx again carried out attacks on the site of an important Indonesian institution, the Police. A number of police personnel data was breached. This leak is known from one of the uploads of the Twitter account @son1x777 which also defaced the BSSN website.

[3] Grace Nadia Chandra, 'Gov't Launches Investigation After Data of 1.3m Reportedly Leaked from Its Covid-19 Tracking App'' (Jakarta Globe, 31 August 2021) <https://jakartaglobe.id/tech/govt-launches-investigation-after-data-of-13m-reportedly-leaked-from-its-covid19-tracking-app> accessed 28 January 2022.

[4] According to Indonesian Civil Administration Law, Personal Data is personal information that is stored, maintained, and kept true and must be treated with confidentiality. Individual data and residence documents must be kept confidential by the State. In general, GR 71/2019 has further expanded the definition of personal data to include data about a person either identified and/or can be identified separately or combined with other information either directly or indirectly through electronic and/or non-electronic systems. Specifically, MoCI Reg 5/2020 defined specific personal data as health data and information, biometric data, genetic data, sexual life/orientation, political views, child data, personal financial data, and/or other data ("**Personal Data**").

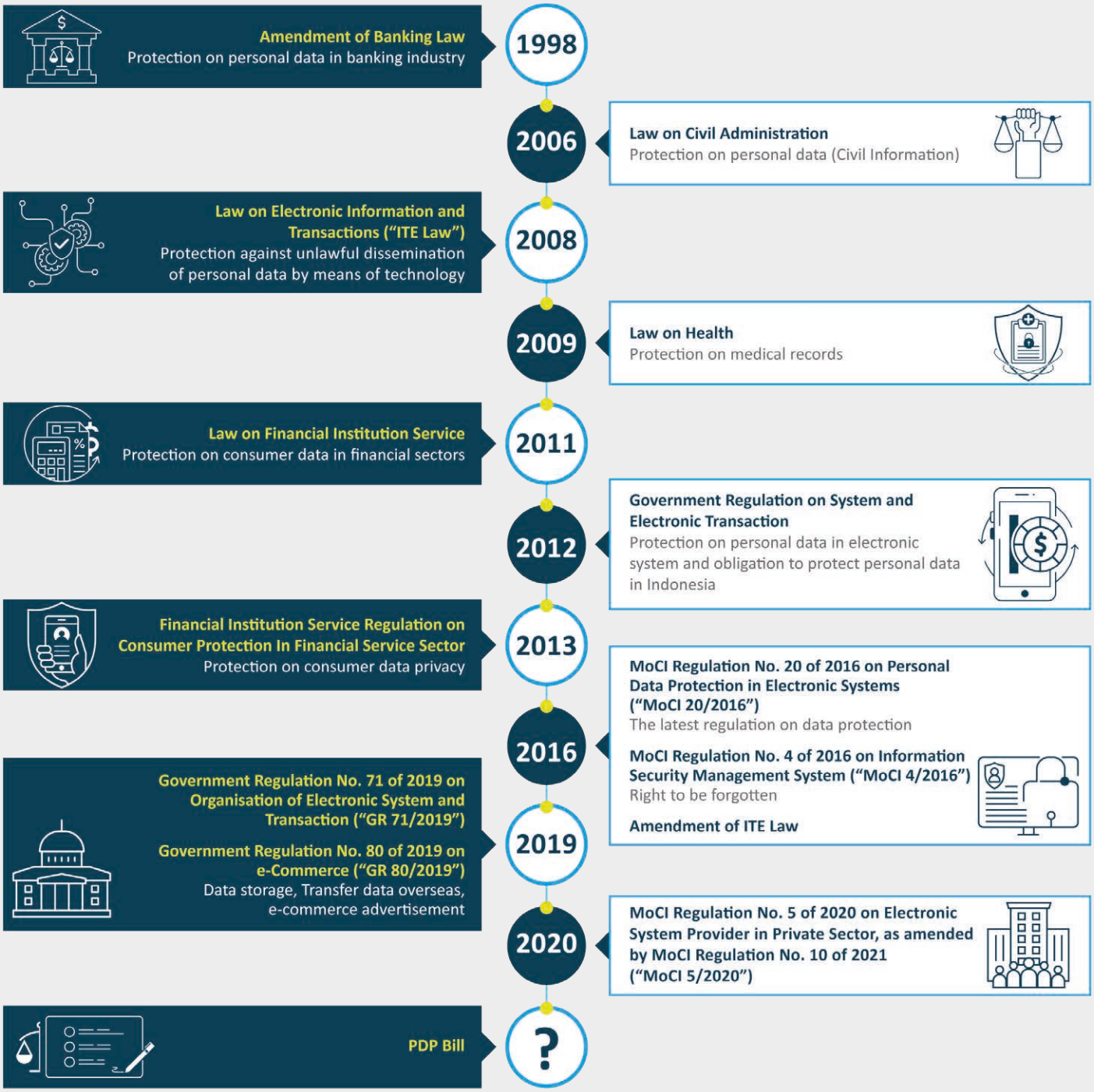
[5] According to Article 1 paragraph (6) letter a of ITE Law, Electronic System Provider is defined as any person, state administrator, business entity, and community that provides, manages, and/or operates Electronic System individually or jointly for the needs of the users and/or other parties ("**ESP**").

WHERE IS DATA PROTECTION REGULATED IN INDONESIAN LEGAL FRAMEWORKS?

Under Article 28 (g) of the 1945 Constitution of the Republic of Indonesia, it is regulated that every person shall have the right to protection of his/herself, his/her family, honour, dignity, and property, and the right to feel secure against and receive protection from the threat of fear to do or not do something that is a human right. This provision is in line with the Universal Declaration of Human Rights which claims that *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."*

PERSONAL DATA PROTECTION PROVISIONS

Regulated under Indonesian Laws and Regulations



PERSONAL DATA PROTECTION BY ESP

What regulations are currently imposed on ESPs (public and private) to protect our Personal Data?

GENERAL OBLIGATIONS

MOCI 20/2016

An ESP must have its own internal regulation regarding Personal Data Protection that conforms with the provisions of laws and regulations as a precautionary measure to avoid failure to protect personal data under its management.

MOCI 5/2020

An ESP must have regulation on electronic information and/or documents, and the regulation must contain the following provisions:

- obligations and rights of electronic system users to use electronic system services;
- obligations and rights of ESP to carry out electronic system operation;
- provisions for liability for electronic information and/or electronic documents uploaded by users of the electronic system; and
- availability of facilities and services and solutions to complaint.

GR 71/2019

An ESP must operate an Electronic System which fulfills the minimum requirements as follows:

- able to redisplay electronic information and/or a document as a whole in accordance with the retention period determined by laws and regulations;
- able to protect the availability, integrity, authenticity, privacy, and accessibility of electronic information in the Organisation of the electronic system;
- able to operate in accordance with the procedures or guidelines in the Organisation of the electronic system;
- equipped with procedures or guidelines that are announced using a language, information, or a symbol that can be understood by a party concerned in the operation of the electronic system; and
- has a sustainable mechanism to maintain the novelty, clarity and accountability of the procedures and guidelines.

An ESP must disclose the following information to its users:

- the identity of ESP;
- the transacted object;
- the feasibility or security of the electronic system;
- procedures for device utilisation;
- contract terms;
- procedures for reaching agreement;
- privacy and/or protection of personal data guarantee; and
- phone number of the complaint centre.

STANDARD SECURITY MANAGEMENT INFORMATION

GR 71/2019

An ESP must facilitate a security system that covers the procedures and prevention and control on any threat and attack that causes disturbance, failure, and loss. Further, the elucidation of the paragraph states that "prevention and control system" includes antivirus, anti-spamming, firewall, intrusion detection, prevention system, and/or management of information security management system.

MOCI 4/2016

An ESP that implements a strategic and high electronic system is required to apply for the SNI ISO/IEC 27001 standard while an ESP that operates a low electronic system is required to apply for the information security index guidelines.

A Strategic ESP and high ESP must have an information security management system certificate while a low-level ESP may have an information security management system certificate.

GR 80/2019

Both domestic and overseas Commerce through an Electronic System Providers ("**CESP**") are required to use an electronic system that has an electronic system eligibility certificate in accordance with the provisions of the legislation.

Domestic and/or overseas CESPs must fulfill the technical requirements stipulated by the MoCI and obtain a reliability certificate in accordance with the provisions of the legislation.

Domestic and/or overseas CESPs are obligated to maintain a safe, reliable, and responsible electronic system and build trust in the system they administer to the public. Domestic and/or overseas CESPs are obligated to provide electronic system security which includes procedures and systems for prevention and countermeasures against threats and attacks that cause disturbances, failures, and losses.

The electronic system security may include security on the computer system side of the domestic and/or overseas CESP as well as on the side of the communication channels used and organised by other parties.

The party who stores personal data must also have a proper security system to prevent leakage or prevent any unlawful processing or utilisation of personal data and be responsible for any unexpected loss or damage that occurs to the personal data .

DATA PROCESSING

GR 80/2019

Personal data must be processed in accordance with the purpose of its acquisition and designation and must not be held for longer than the required time. It must be processed in accordance with the data subject rights as regulated in the laws and regulations.

MOCI 5/2020

If the ESP that manages, processes, and/or stores electronic data or electronic systems is outside of the Indonesian territory, the ESP must provide access to the electronic data or electronic systems for the purposes of enforcement of criminal law involving:

- an Indonesian citizen; or
- a Business entity established under Indonesian law.

MOCI 20/2016

Data processing (acquisition, collection, processing, analysis, storage, display, announcement, delivery, dissemination, and erasure of personal data) carried out by an ESP must be based on the principle of good personal data protection as follows:

- due regard to personal data as privacy;
- personal data is confidential in nature in accordance with the consent and/or based on the provisions of laws and regulations;
- based on consent;
- relevance with the purpose of acquisition, collection, processing, analysis, storage, display, announcement, delivery, and dissemination;
- worthiness of the electronic system that is being used;
- good faith to immediately notify Personal Data Owner in writing as regards any failure on personal data protection;
- the availability of internal regulation for the management of personal data protection;
- responsibility for any personal data that are under the possession of users;
- ease of access to and correction of personal data by Personal Data Owner; and
- integrity, accuracy, and validity, as well as updates of personal data.

GR 71/2019

An ESP has to implement the following principles in connection with the processing of the personal data (acquisition and collection, processing and analysis, storage, fixes and updates, appearance, announcement, transfer, dissemination, or disclosure, and/or deletion or destruction):

- Personal data collection is conducted in a limited and specific manner, legally valid, fair, with consent and agreement of the Personal Data Owner;
- Personal data processing is conducted in accordance with its intention;
- Personal data processing is conducted by ensuring the rights of the Personal Data Owner;
- Personal data processing is conducted accurately, completely, not misleading, up-to-date, accountable, and taking the intention of personal data processing into consideration;
- Personal data processing is conducted by protecting the personal data security from loss, misappropriation, access and illegal disclosure, as well as alteration or destruction of personal data;
- Personal data processing is conducted by notifying the purpose of collection, processing activities, and failure in protecting personal data; and
- Personal data processing is destroyed and/or deleted unless in a retention period in accordance with the need based on laws and regulations.

DATA TRANSFER

MOCI 20/2016

Prohibits the transfer of personal data to another country or territory outside Indonesia unless such countries or territories have been declared by the Minister of Trade as having an equal standard or level of personal data protection to that in Indonesia.

MOCI 20/2016

Transfer of personal data in electronic system can only be done with the consent of the Personal Data Owner, unless otherwise specified by the provisions of the legislation and after verification of accuracy and conformity with the purpose of data collection and collection of the personal data.

In terms of cross-border transfer of personal data which is conducted by an ESP who is domiciled in Indonesia, such data transfer must:

- be in liaison with the MoCI or appointed officials. Such coordination is in the form of reporting the plan of transfer of personal information, at least contain the clear name, designated country, recipient name, implementation date, and reason/ purpose of the transfer;
- report the result of such transfer of personal information; and
- implement the laws and regulations regarding the transboundary exchange of personal data.

GR 71/2019

Data processing that includes the transfer of data to obtain valid consent from the Personal Data Owner for one or several specific purposes that have been submitted to the Personal Data Owner.

Personal data processing must meet the necessary conditions to:

- fulfill agreement obligations in the event that the owner of the personal data is a party or to fulfill the request of the owner of the personal data at the time of entering into the agreement;
- fulfill the legal obligations of the personal data controller in accordance with the provisions of the legislation;
- fulfill the protection of the legal interest of the Personal Data Owner;
- exercise the authority of the personal data controller based on the provisions of laws and regulations;
- fulfill the obligations of the personal data controller in public services for the public interest; and/or
- fulfill other legitimate interests of the personal data controller and/or the Personal Data Owner.

The elaboration above shows that provisions on Personal Data are regulated under several laws and regulations in Indonesia. There is, however, no consistent legal framework on their implementations.

The inconsistency and the overlap between the obligations of the parties involved inhibit law enforcement on violations against Personal Data, which at the end of the day lead to inadequate protection for the Personal Data of Indonesian citizens whose awareness of the importance of Personal Data protection needs improving.

PERSONAL DATA LEAKS, WHO IS RESPONSIBLE?

Should a data leak occur, an ESP is obligated to notify the Personal Data Owner in writing of its failure to protect the confidentiality of Personal Data in the Electronic System it manages. The user has the right to file a complaint against ESP and to resolve the Personal Data dispute. The user is also entitled to gain access or opportunity to change or update and obtain their Personal Data that has been submitted to ESP without disrupting the Personal Data management system unless otherwise stipulated by the provisions of laws and regulations. In addition, the user can request the destruction of his/her certain individual data in the Electronic System managed by ESP.

e-HAC's case

The Peduli Lindungi App, which provides COVID-19 vaccine e-certificates, requires its users to input their cellular phone numbers and five other pieces of information (name, National Identity Number ("**NIK**"), date of birth, date of vaccine and type of vaccine). However, users are no longer required to input their cellular phone numbers. President Joko Widodo's vaccine certificate in the application was accessed using information concerning his NIK and COVID-19 vaccine date, and the information on his vaccination can be found on the mass media.

The vpnMentors researchers have notified the MoH, the Indonesia Security Incident Response Team on Internet Infrastructure ("**ID-SIRTII**"), and the Computer Emergency Response Team ("**CERT Indonesia**") of the data breach on e-HAC. However, the reports were reportedly met with an absolute silence. The MoH as the data controller and processor should be responsible for the integration of data utilisation on e-HAC and Peduli Lindungi App with a national data centre in the interests of data security. The Government is obliged to facilitate information technology and electronic transactions to protect public interest from any type of disturbances due to any misuse that disrupts public order.

The BSSN as the authorised institution performing cyber security technical policy must be responsible for recovery and cyber security risk management. The Ministry of Communications and Informatics ("**MoCI**') as the regulator has the obligation to take strategic steps in updating data protection governance in PeduliLindungi App system under the prevailing laws and regulations.

The latest news we obtained from various sources confirmed that e-HAC servers were quietly shut down on 24 August 2021, and the authorities have called off their investigation into the alleged leak of e-HAC data after seven days of investigation on the grounds that *"even if the data leak did occur as confirmed, it would be impossible to hold the perpetrators to account because Indonesia does not have a regulation on data protection".* The MoCI has performed a migrating system from Peduli Lindungi App to the National Data Centre covering system migration, application services and application database. Migration was also performed on SiLacak Application System and **PCare** Application System on 28 August 2021.

These notable cases prove that ESPs neither notify users of the leaks nor can the users exercise their rights because the leaks have always been denied, unsolved and as a result, the perpetrators go unpunished.

Susanto
Head of KPAI

"There has been a leak on KPAI's database and such incident has been reported to Directorate of Cyber Crime, Indonesian Police Headquarters and BSSN to coordinate and to decide the next step to conduct mitigation of data protection security. KPAI had taken steps to keep its data secure, claiming that the incident did not affect its complaint system."

Ade Ahmad Nasution
BRI Life Corporate Secretary

"The hacker had gained access to the BRI Life Sharia Insurance data system, which held the details of around 25,000 individual sharia insurance policies, but added that it did not affect the data of other companies within the BRI group. This incident had no effect on other BRI customers and other companies within the BRI group."

Johnny G. Plate
Minister of Communications and Informatics

"Tokopedia has explained that user accounts and financial data are safe. It was conveyed [during the meeting that Tokopedia's] security system cannot be breached, although data relating to names, emails and telephone numbers may have partly been accessed by hackers. Tokopedia is conducting an in-depth evaluation."

"The agency was still conducting an investigation to ensure that no data was stolen, adding that pusmanas.bssn.go.id had been temporarily disabled."

Anton Setiyawan
BSSN spokesperson

"Following the probe by the National Police at the Health Ministry and its partners, [we] did not detect any attempts to retrieve the data stored on the e-HAC server" seven days after investigation on the alleged leak of e-HAC data was called off.

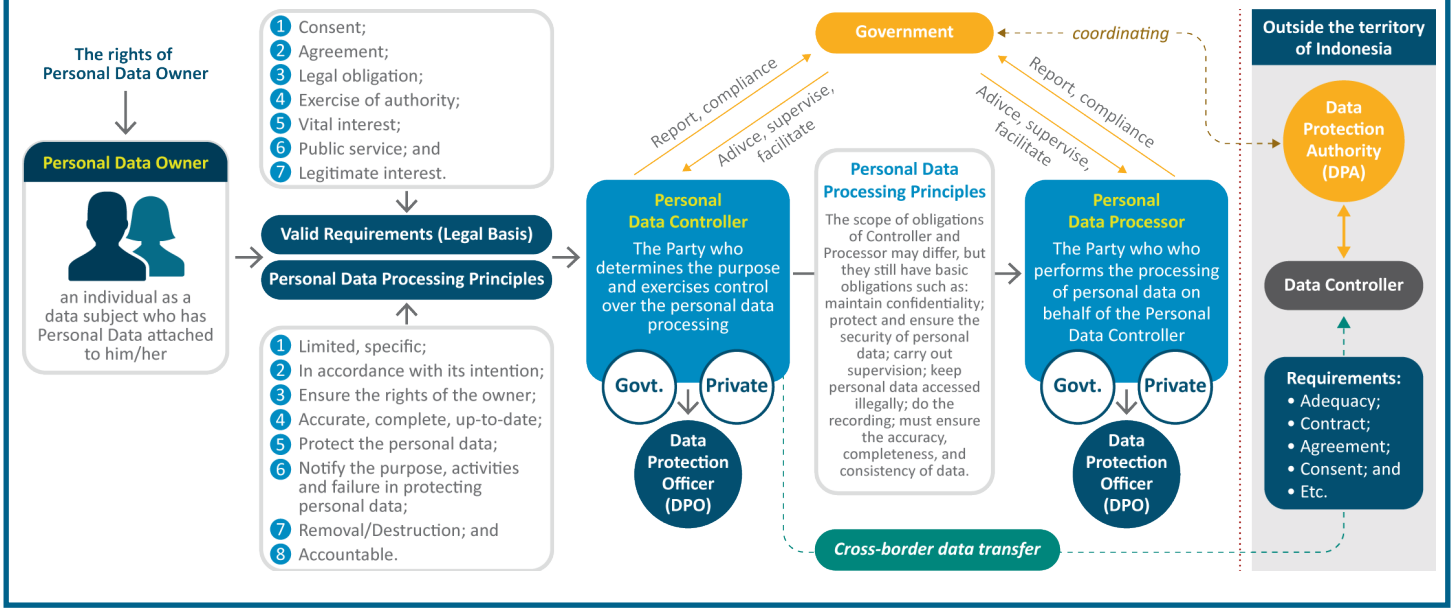
Insp. Gen. Argo Yuwono
National Police spokesman

INDONESIA PDP BILL – LATEST UPDATE

Even though the PDP Bill was drafted back in June 2019 and has been approved by President Joko Widodo, it is still under discussion in the House of Representatives. The prolonged discussion seems to show that the low awareness and accountability of ESP in Indonesia are not yet worrying enough.

To keep up with the pace of digital transformation and to prevent further losses on a user's side when a data breach occurs, PDP Bill sets out tighter and stricter provisions for data processing process. Generally, the new PDP concepts regulated in the PDP Bill are as follows:

THE NEW CONCEPT OF PDP IN THE PDP BILL



Considering the lengthy discussion on the PDP Bill and the vast development of cyber world, many experts started questioning the comprehensiveness of the PDP Bill and whether its provisions are in accordance with those in the General Data Protection Regulation ("**GDPR**").

The PDP Bill entitles data owners to regulate and process their own Personal Data, except when needed for state defence and security issues, law enforcement, state administration, financial and monetary supervision, payment system and financial system stability. Such exceptions provide the Government with unlimited access to Personal Data. In this matter, the Government should be obligated to give reasonable grounds for such access.

In the event of national defence and security for instance, there must be an urgent situation that forces the Government to access Personal

Data. There is a risk of the Personal Data being used for political even economical purposes especially when there is no warranty that the data will not be used for any other purposes or disclosed to any unauthorised parties. Moreover, considering the rampant leak of cases which happened on the Government's database and website, there will still be no guarantee that our Personal Data is safe in the Government's hand.

In the PDP Bill, every Personal Data Owner is entitled to withdraw consent for his/her Personal Data processing that has been given to the Personal Data controller. The withdrawal is performed at the latest 3 x 24 hours since the Personal Data controller receives withdrawal request for Personal Data processing. However, in this matter there is neither a provision nor a guarantee on whether withdrawing consent could be as easy as providing it.

As for overseas data transfer the PDP Bill states four mechanisms with no particular order of importance. The GDPR prioritises the mechanism for adequacy decision, appropriate safeguards and binding corporate rules to safeguard overseas data transfers. In the absence of clear arrangement of data protection authority that will be mandated as a party in charge of ensuring appropriate level of protection before the data transfer can be conducted, the Personal Data controllers or processors may pick a mechanism at their convenience. However, such discretion is most unlikely to favour the interests of the Personal Data Owner.

Then comes the root of the postponement of the issuance of PDP Bill. Supervisory authority of PDP. The PDP Bill states that the implementation of PDP in Indonesia will be conducted by the Government, under the MoCI, which will have the authority to regulate Personal Data processing, receive reports on data personal breaches, impose administrative sanctions for non-compliance, and implement Government measures for PDP. With the immunity possessed by the MoCI against the PDP Bill, which serves as a regulator, supervisor and processor of Personal Data, surely the conflicts of interest will arise.

On the other hand, the Lawmakers (House of Representatives) have insisted that the proposed supervisory authority be independent of the Government to avoid any possible conflict of interest. There are always serious obstacles in establishing an independent authority. Presently, the Government is aggressively fighting against COVID-19 pandemic, and consequently spending a large amount of money now would not be considered prudent.

Henri Subiakto, Expert Staff of the MoCI stated that the Government stand points are *"if there will be a new supervisory body mandated by law, in this case the PDP Bill, then the appointment and election of the officials for the supervisory body must be done by means of a presidential regulation and not based on a decision by the House of Representatives as doing so will weaken the presidential system in Indonesia. If necessary, the President will be authorised to form it and responsible for the performance of the institution. The new independent agency has become an issue in almost every law on the grounds that the independence of supervisory and law enforcement agencies is considered overlapping. Law enforcement institutions are considered to have existed. The state auxiliary institution actually disrupts the presidential system. Administrative enforcement does not have to be carried out by a separate agency as sectoral supervisory institutions also exist with systems that are already running, for example the banking and financial services sector (there are Financial Services Authority or Otoritas Jasa Keuangan (OJK) and Bank Indonesia (BI). Finally, the MoCI is also considered to have resources that are responsible for digital transformation issues. According to him, when dealing with other countries, or international institutions, and global corporations, the government already has a credible network and adequate facilities."*

Independent supervisory authority is considered as an effective feature that has been adopted by many countries around the world that impose modern PDP Law. Out of 143 countries that have PDP Law, only 10 countries which data protection authorities are not independent. Some of these countries are in Asia, and Taiwan is the only country that claims to have rules for public sector privacy without independent data protection authority. However, the country is exploring the possibility to establish one. In order to be beneficial for citizens and businesses, the decisions made by data protection authority must be independent of direct and indirect external influence from the government and private sector.

SO WHAT'S NEXT?

With the Government constantly promoting the digitalisation in almost of all aspects of life, from the 4.0 industrial revolution program to booster for unicorn and decacorn digital start-ups, low awareness of the importance to protect Personal Data of its citizens has made major government websites and ESPs vulnerable to cyberattacks. Cyberattacks affect not only the systems of ESP but also the integrity, security, and confidentiality of the public's personal information. It violates citizens' human and privacy rights and endanger the security of the State.

From a business perspective, the well-equipped and independent supervisory authority is the prerequisite of the certainty in compliance with the law, consistency in law enforcement, key aspects in healthy competition and the credibility as a neutral mediator in resolving Data Protection conflicts effectively. Not only is independent data protection authority beneficial for business, but it is also important for the confidence of public in general. The public will trust the system, and they can access to inquire and file complaints without going through long and tiring legal proceedings. This authority also serves as a mediator between individuals and businesses to find the appropriate solutions out of court.

It is therefore necessary to consider establishing an independent data protection authority in Indonesia to help ensure legal certainty and to adapt to conditions of economy and technology that continue to develop. It can also design public guidance to ensure uniformity of interpretation and application of regulations across the country. By establishing the independent authority, Indonesia can also participate in international enforcement cooperation's in terms of Data Protection issues through various independent supervisory networks. Independent and well-resourced data protection authority can be the key to attract foreign investments particularly in the fast-growing digital/data era. The closer the Indonesian Data Protection Law to the international standard, the easier it is for companies to cooperate with Indonesia effectively.

The PDP Bill states that data privacy protection constitutes a human right. It is therefore reasonable to place the bill that includes the supervisory authority of data privacy protection within the framework of human rights enforcement. Both the government and the House of Representatives must immediately settle the debate over the supervisory authority. Neither should be shackled by conflicting opinions as the privacy of Indonesian citizens' Personal Data are put on the line.

If you have questions or require any additional information, please contact Jade Hwang Poh Geok, Andina Sitoresmi, Randyaz Iskandar, David Septian Lienardo and Hillary Tjandra of Roosdiono&partners (a member of ZICO Law).

Jade Hwang Poh Geok
Foreign Counsel

jade.hwang@zicolaw.com
t. +62 21 2978 3888

Jade is an experienced corporate lawyer specialising in cross-border M&A, joint ventures and corporate restructuring. She is also well-versed in advising capital market and securities law.

She has substantial experiences in technology, real estate, energy & resources, agriculture and financial institutions sectors across ASEAN region representing multinationals, Asian companies and investors ,and government-linked companies. Her regional practice experiences includes being a resident in Malaysia, Cambodia and currently Indonesia.

Andina Sitoresmi
Senior Associate

andina.sitoresmi@zicolaw.com
t. +62 21 2978 3888

Andina's expertise includes advising clients in corporate secretarial compliance, legal due diligence exercises and assisting in establishing businesses in various sectors in Indonesia. Andina has acted for major corporations on domestic and cross border investments, specifically in CMT, hospitality and medical services sector. Andina is also an Intellectual Property (IP) specialist in Roosdiono & Partners.

Randyaz Iskandar
Senior Associate

randyaz.iskandar@zicolaw.com
t. +62 21 2978 3888

Randyaz' experience includes advising clients in corporate and commercial transactions and assisting them in establishing businesses in various sectors. He has acted for major corporations on domestic and cross border investments and M&A in various sectors such as plantation, financing, mining, health, manufacturing, pharmaceutical, IT, hospitality, and aviation.

He has also been involved in several high-profile financing deals and commercial litigation matters.

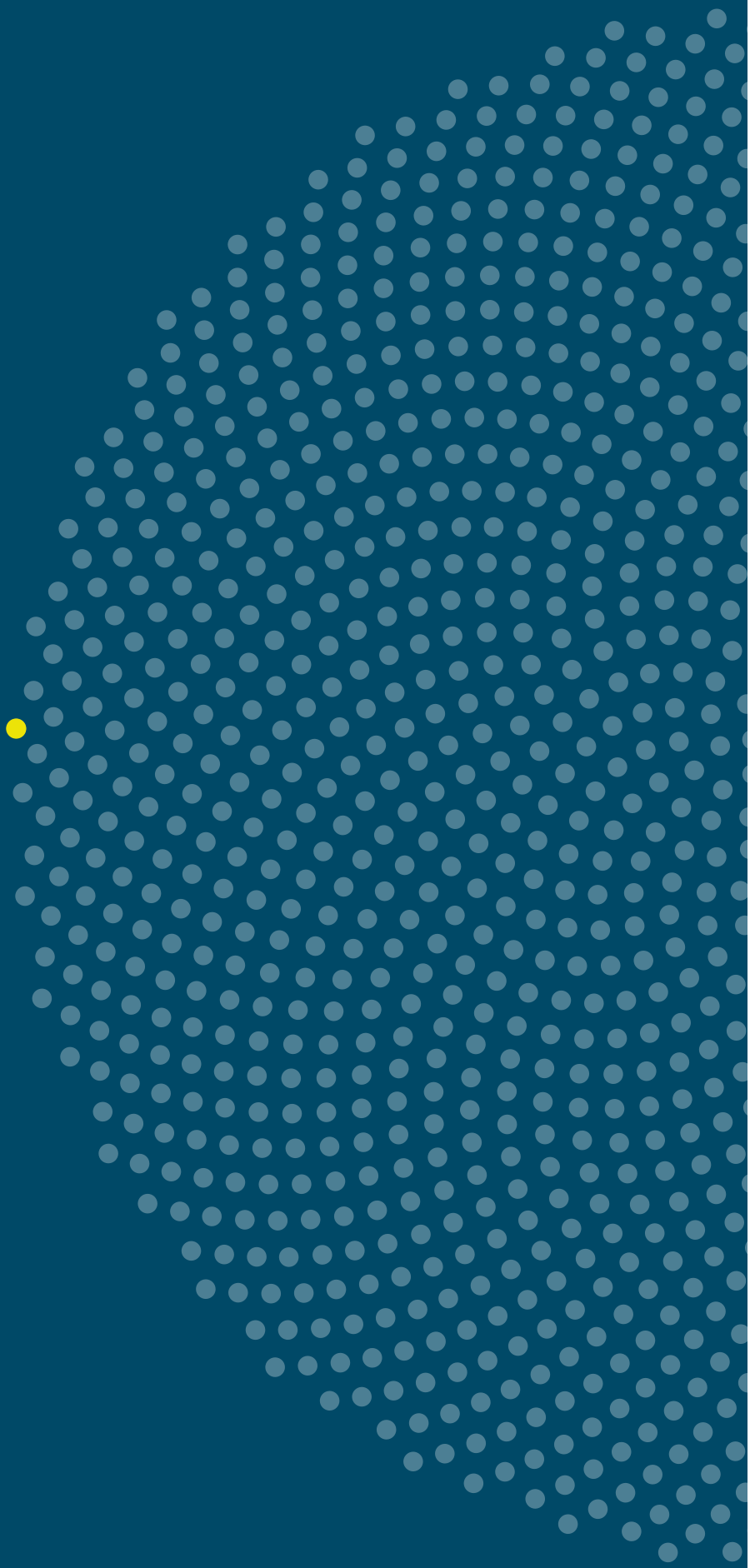
This article was also assisted by David Septian Lienardo and Hillary Tjandra of Roosdiono&partners (a member of ZICO Law).

This article was edited by ZICO Law Knowledge Management & Training.

This article is updated as at 28 January 2022. The information in this article is for general information only and is not a substitute for legal advice. If you require any advice or further information, please contact us.

ZICO | law

ASEAN INSIDERS,
by origin and passion



ASEAN 10/10

BRUNEI | CAMBODIA | INDONESIA | LAOS | MALAYSIA
MYANMAR | PHILIPPINES | SINGAPORE | THAILAND | VIETNAM