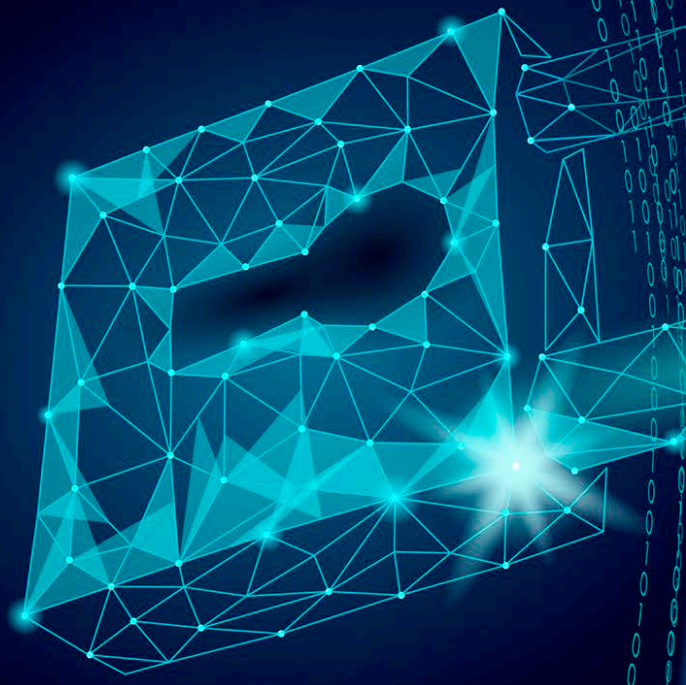
KPMG

Data Privacy as a way of life

Indonesia Edition



December 2020

home.kpmg/id

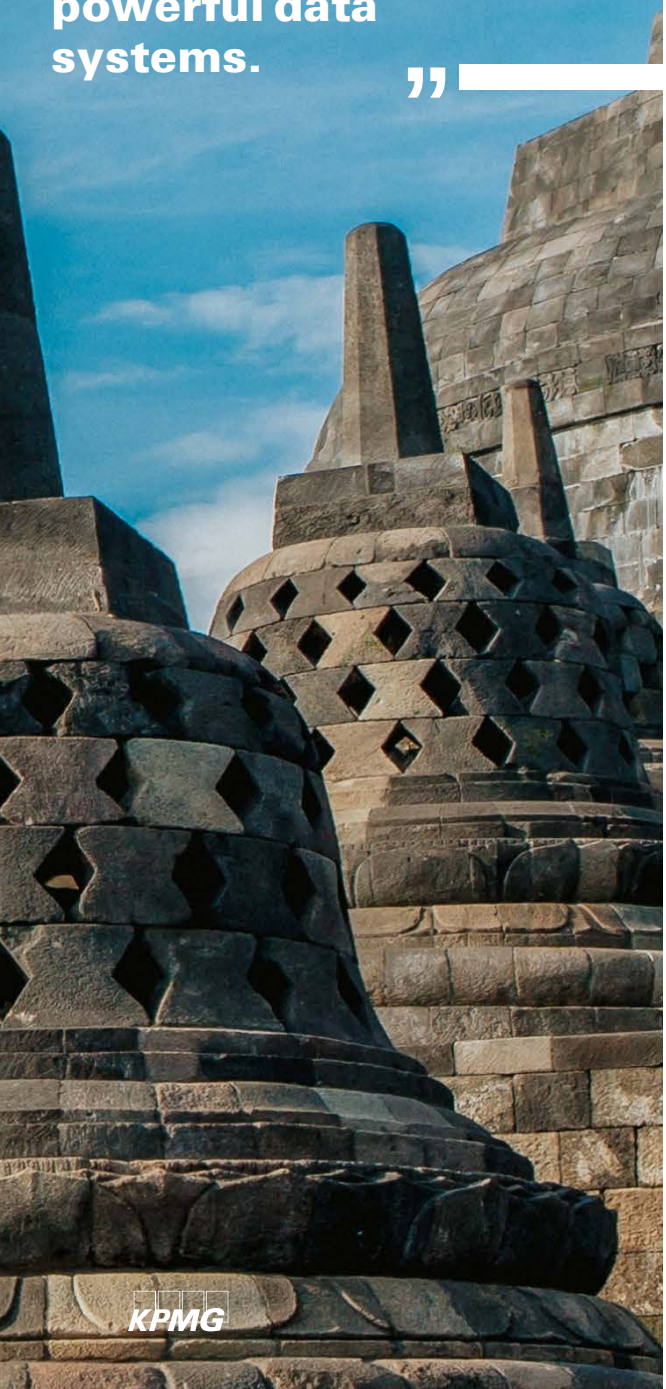
Nurturing a privacy-conscious culture

The digital transformation trend across industries has spawned an unprecedented appetite for personal data. For most enterprises, personal data is the key ingredient to a successful digital initiative. Collectively or otherwise, this data can provide an understanding of the user in terms of preference, perception, personality, identity and even, certain identifiable economic or social cohorts. These insights are a key to most digital initiatives that attract and extend user engagements and experience.

If done properly and legitimately, leveraging personal data can benefit both the individual and enterprises. However, at present, the collection and use of such data is done surreptitiously, without the permission of the individuals The are incidents reported frequently on privacy intrusion, misuses of personal information and failure to adequately protect personal data have increased the mistrust amongst individuals.

“There is a danger of treating the privacy bill as a ‘tick the box’ compliance activity, rather than a deliberate move towards a culture where transparency, citizens’ rights and accountability are second nature.”

“Viewing personal data as an asset opens the door to exciting, value-creating investments, accelerating a shift to simpler, less costly and more powerful data systems.”



In Indonesia, the need to protect personal data is even more important. The country’s high level of mobile penetration and internet connectivity suggests a pervasive amount of personal data available digitally, which, if abused, could lead to lasting impact to the country’s largely young population and threaten the country’s digital ambition.

The upcoming Personal Data Privacy (“PDP”) Bill is need of the time. As noted by Bapak Semuel Abrijiani Pangerapan, Directorate General of IT Application at Ministry of Communication (MOCI), the PDP not only regards “data privacy as basic human right” therefore enshrining protection of personal data. More importantly, the bill provide the proper and legitimate means for the collection, storage and usage of personal data and therefore should be viewed as the fundamental building block for any digital transformation initiatives where personal data is leveraged.

For organizations, the PDP Bill brings Indonesian personal data privacy practices to international standards by setting forth requirements of notification, disclosure, rights of erasure and data privacy officers (DPO). According to Bapak Semuel, these requirements are not defined for perfunctory compliance (tick the box exercise) by organization. They should be viewed as management practices meant to develop a more privacy-aware culture within the organization and strengthen the organizational sense of responsibility for the personal data entrusted to it.

Five issues to consider

01 Put customers and employees at the heart of your privacy strategy

Data privacy regulation is a step towards becoming a true digital economy. Protecting the informational privacy is not only the right thing for any responsible organization to do but it also helps gain trust and enhance the organization's prospects for lasting success. Privacy failures could be very damaging to the organization's reputation. It will earn the trust of the stakeholder which will pay dividends in terms of those stakeholders' loyalty and their contribution to its success.

It's more important to begin to instill the right habits and behaviors, so that everyone in your organization appreciates customers' rights to privacy and choice. In order to help build and cement trust, your business should make customers aware of what kinds of personal information you hold and how you use it, with transparency and accountability as your guiding principles. Customers are entitled to know what is being done with their personal information - and expect you to tell them. This means understanding the customer journey and making privacy an essential feature of that journey - and an integral part of your wider business strategy.

And as you map the customer journey, it's the touchpoints that should receive the highest priority. These are the public-facing aspects of your business, like handling customer complaints and queries, or targeting individuals with personalized offers. In an omni-channel world, where customers interact via phone, apps, online chats, email and post, these touchpoints need to offer a consistent experience. Touchpoints offer an ideal opportunity to showcase transparency, and to explain how you're using customers' personal data responsibly. By paying close attention to the quality and integrity of such interactions, you can present a positive picture of how your organization manages privacy, in the process enhancing your reputation with customers and employees, and reassuring regulators.

You may want to introduce incentives that encourage appropriate values and behavior. And you'll certainly want to nurture an environment where any risks and issues can be discussed openly, and processes challenged where necessary. Training and communications can help spread the word and equip employees with the skills and awareness of privacy issues.

02 Understand that data is an asset and a liability

As it has been mentioned, the new PDP Bill is not simply a static deadline. It's part of a journey towards better management and use of that most valuable resource: personal data.

The potential liability of data derives not just from the clearly articulated the penalties, but also from any loss of customer trust and brand and reputational damage resulting from a breach and/or unacceptable behavior.

On the flip side, viewing data as an asset opens the door to exciting investments that can create value: transforming the operational infrastructure and accelerating a wider and longer-term shift to simpler, less costly and more powerful data systems.

All of which should help enable your organization to not only gain more confidence in its privacy capabilities; but to also enhance other functions that depend heavily on customer data, like fraud detection, marketing and customer analytics.

You may also want to think about the skills you have within your organization. In addition to lawyers and compliance and risk professionals, you need access to technology and data experts who can help you embed the PDP Bill as part of your overall data strategy.

03 Don’t rush into major technology investments

In the push to be ready, it’s tempting to believe that privacy software solutions can ensure compliance. In reality though, without a clear privacy strategy and documented roadmap, and a pre-existing culture of transparency, technology may simply add more complexity — at considerable cost.

By concentrating on activities that will add value to your privacy efforts and by seeking advice from knowledgeable experts, you should have a better chance of making the right technology choices. Don’t forget that privacy regulations will continue to evolve, so avoid large investments today that may leave you with something that isn’t fit for tomorrow.

Before considering which solutions to invest in, you must first get the basics right — starting with strong privacy governance. Once a simpler, more streamlined set of processes and roles are in place, you can then seek the appropriate

04 Be prepared for questions

Privacy is a hot topic and only likely to get hotter. Reputational damage — as a result of breaches or unethical activity — can be immense, and there is a small but growing community of journalists and other stakeholders that are eager to ask

difficult questions. The answer is to be media ready at all times, with a well-briefed communications team and a senior, credible, privacy-aware spokesperson/people.

When dealing with customers, it’s vital that all staff are fully trained and able to anticipate questions. It only takes one poor or uninformed response — especially where a customer has a good understanding of her/his rights — to create a negative experience, as well as an investigation.

05 Regulatory challenges on data residency

Any company dealing with data from Indonesia, data subjects needs to comply with the PDP Bill, and the globalization of business means that many organizations are likely to handle such data in some form — even if this means just one customer or employee. The privacy bill impacts collection, use and disclosure of data, on a global scale, for organizations outside of the Indonesia, which is likely to have considerable impact.

With today’s international organizations typically involved in a complex web of subsidiaries and outsourced providers, the onus is on your data controller to ensure that every part of the value chain applies the same high standards of privacy. And it’s not just about customers; employees in the Indonesia also fall under the PDP Bill. Any financial, health and other sensitive, personal information needs to be handled in a way that meets the new standards. You will probably have to align any human resources (“HR”) systems with relevant PDP Bill.

KPMG conducted a discussion with the one of the senior government officials – Mr. Semuel Abrijani Pangerapan, B.Sc, Directorate General of IT Application – Ministry of Communication and Informatics ("MOCI") with regards to the government's preparation for the Personal Data Privacy Bill. Below are the some of the thoughts shared on Data Privacy readiness and challenges in the country.

Semuel Abrijani Pangerapan, B.Sc

Our neighboring countries already have established the data privacy law, why is it important to have a personal data protection law in Indonesia?

In the digital era, the Personal Data Protection Bill is an important regulatory framework capable of protecting personal data in doing transaction and interaction in the digital space.

The strategic role of data, which generally contains personal data, makes personal data vulnerable to be misused, therefore a regulatory framework that regulates the management of personal data usage is needed.

Talking about the Indonesian context, the protection of personal data is a basic human right, which is mandated in the UUD 1945, especially article 28G paragraph 1 and article 28H paragraph 4.

Therefore, in reference to the UUD 1945, the Indonesian PDP Bill is here to ensure an important role of the state in protecting its citizens' personal data.

Currently the regulations regarding personal data protection in Indonesia are still scattered in more than 30 different sectoral regulations, so it is necessary to formulate a regulation on personal data protection that is comprehensive.

With the existence of a comprehensive PDP regulation, it is hoped that the public will become more aware and understand the importance of data privacy.

In the international context, the nature of data flows that do not recognize geographic boundaries requires a regulatory framework capable of bridging cooperation in protecting the personal data of the Indonesian people, both within the territory of Indonesia and outside the territory of Indonesia.

How critical is the role of senior management to drive the privacy culture in an organization?

I think by looking at the level of awareness of the majority of Indonesians regarding data privacy and digital literacy, the role of senior management in the organization is crucial to foster the awareness.

The PDP Bill also hints at the importance of an organizational culture that is aware of the importance of data privacy. This is marked by the obligation for data controller and data processor to have data protection officer (DPO), where DPOs in each organization are tasked to disseminate information about data privacy, build privacy culture and oversee the personal data management mechanism to comply with the Indonesian PDP Bill.

What do you think are the key challenges for the authority for the compliance of this law?

As I mentioned earlier, in general, the level of awareness of the Indonesian population for data privacy and data literacy is still at a low maturity stage. We have gradually introduced the topic of data privacy and increased the quality of our digital literacy programs for the society, along with stakeholders, from top to bottom levels. At the top level we focus on directly increasing people's digital literacy; at the middle level we focus on technological interventions that create safer and more comfortable digital space; while at the bottom level we focus on partnerships with law enforcement officials.

However, I personally think that increasing the awareness of Indonesian human resources in understanding data privacy and digital literacy will remain a big "homework" that we must continue to monitor and work on together.

From the regulatory perspective, the key implementation of the Indonesian PDP Bill lies in the formation of the DPA (data protection authority. For the business sector and organizations, the presence of DPOs is also an important requirement.

What are your thoughts on an effective data privacy strategy?

There are 3 keys to a personal data protection strategy, namely human resource capacity, technology intervention, and regulatory support.

It is crucial to increase the digital literacy of the society because no technology can function without human interference. Without digital literacy, the risks associated with technology cannot be mitigated. In terms of protection of personal data, apart from being a subject whose rights are protected, users can also actively exercise their rights as owners of personal data. Therefore, it is necessary to have human resources with understanding of the concept of data privacy and digital literacy.

Technological intervention talks about how we can produce innovative products that adhere to the concept of "privacy by design". This concept means technology manufacturers always prioritize the importance of data privacy in designing detail of the technological product developed and its features. The cases of misuse of personal data have encouraged several global tech giants to adopt this concept and change their approach in producing new features in their technology products.

PDP regulation is the final pillar of an effective PDP strategy considering that the legal framework is needed to provide guidelines for the public in managing personal data, as well as to regulate the mechanisms for sanctions that can be imposed on misuse of personal data cases.

When organizations are embarking on digital transformation, what are the considerations, an organization should take for privacy and data protection?

In digital transformation, we certainly cannot be separated from the activity of data processing, including personal data processing. Therefore, it is important for organizations to understand some of the main principles of transparent and accountable data management, which include: data confidentiality, data security, data control, data access, and data accuracy. The complete understanding of the principles of data management will prevent companies from using personal data that is not suitable for purpose.

Only after organizations have understood the principles of data management, they can move to the next phase of the digital transformation process, which is understanding the technicalities and complexities of digital technology adoption.

What do you consider are the key success factors for data privacy program in Indonesia?

In my view, data privacy protection movement or program required an involvement of several stakeholders, where it can not only be carried out by one or two actors but requires collaborative performance from all parties involved.

Therefore, this data privacy movement or program can be considered successful if all the actors involved, including government, business sector, NGOs, media, academics, and the general public.

Privacy awareness on protecting personal data must be disseminated to all levels (owners, controllers and processors), and all other ecosystem components (law enforcement, civil society, controllers).

How is this data protection law going to mature the data privacy posture in Indonesia in the next 3 to 5 years?

The Indonesian PDP Bill will take full effect two years after this law is passed, with the hope that the two-year period can be used to build awareness of the public and stakeholders, and to start compiling technical guidelines regarding PDP, such as drafting SOPs and code of ethics.

After completing the two-year preparation period, in the third year the Indonesian PDP Bill is expected to be fully effective, in accordance with all the guidelines and sanctions mechanisms

Technically, I also expect that in the third year, many business sectors have started to adopt DPOs, the government already has DPA, and most importantly there is an increase in the public awareness of the importance of data privacy in the digital era.

Will the PDP law draft provide visibility to the risk related to compromise of personal data? Does it have the control framework to protect personal data?

No, the PDP law discusses more about governance not the technical aspect. So, all the responsibility regarding personal data protection lies with the controller of the data. The controllers need to protect the data in their own ways.

Therefore, the things that are regulated such as collecting personal data, collectors must have legal basis such as what they collect the data for, how they get it, and so on. In case if there is any compromise, the collectors are required to immediately report to the data owner, the investigator, and the authorities who are responsible for it.

You must be aware of the personal data breach related to online retail platforms and citizen data. In your opinion, does the PDP law will help in better detection, protection and management of such incidents?

Not directly. The PDP bill will be principal guidance for data controllers in managing if the data breach happens.

Rights and obligations are also given to controllers. Their obligations is to get consents in collecting personal data, protecting and guaranteeing the data they control. If they want to transfer the data, they must understand the mechanism on their own. The technical measures are not given in the law, they must understand by themselves on how to secure it.

Detection and protection are the controllers' business. The specific standard is not explained in the law and should be created by the controllers based on their type of business. Different types of businesses could have different methods in the detection and protection of data breaches. The PDP law will provide guidance.

What is your thought if there is a failure in protecting customer data (like one of e-commerce case) and citizen data (by government)?

Once a data leakage occurs, the data manager is obligated to report it to the authorities and fill out all the forms that must be filled in. It is also obligatory to notify all people who may be affected by the leakage of the data, including the consequences or risks of this leak.

If data breach happens, the form will be audited. The mechanism of audit will be ruled further by the Data Protection Authority (DPA) and data controllers must comply with the determined rules.

Privacy as a source of competitive advantage

With the world becoming more and more sensitive towards the privacy of the individuals, the enactment of the PDP Bill is expected to strengthen country's privacy status as a safe country. Organizations will be required to upskill their staff to perform the business transformation to meet the obligations. Compliance deadlines inevitably focus the corporate mind. But in the case of the PDP Bill, any attempts to meet regulatory obligations should not be at the expense of a long-term strategy that acknowledges privacy as a source of competitive advantage. It is essential that data protection is taken up as a key boardroom agenda to drive wide compliance across organizations. By considering how your organization can meet the needs of customers and employees, organizations can build a privacy-aware culture, and a governance infrastructure, which puts the right information at individual's fingertips and consistently demonstrates transparency. To lead the new privacy regime, it is time, for organizations to rethink their obligations and find new ways to restore stakeholder trust.

Key questions for Boards

- Who is in charge of privacy compliance? Are the right accountability and governance structures in place?
- Are we prepared to speak publicly and to our customers about how we manage their privacy?
- How do I know whether employees are taking an ethical stance towards privacy?
- Do we have a data strategy? Is it focused on what's best for the customer?
- Are we handling our key customer touch points efficiently and appropriately?
- What actions are we taking to nurture a privacy-aware culture to earn and retain our customers' trust?
- Do we view the PDP Bill as a one-off initiative? Or is it part of a proactive risk management approach, enabling us to put our customers at the center of everything we do?

"While the controller has ultimate accountability, the shift in liability for processors reinforces the need for controllers and processers to work closely together, to help maintain the privacy rights of data subjects in line with the PDP Bill."

Contacts

KPMG Siddharta Advisory
35th Floor, Wisma GKBI
28, Jl. Jend. Sudirman
Jakarta 10210, Indonesia
T: +62 (0) 21 574 0877
F: +62 (0) 21 574 0313

Irwan Djaja
Partner In Charge Advisory Services
Irwan.Djaja@kpmg.co.id

Benson Tran
Head of IT Assurance and Cybersecurity
Benson.Tran@kpmg.co.id

Freddie Mulyadi
Director, IT Assurance and Cybersecurity
Freddie.Mulyadi@kpmg.co.id

Dhirendra Kumar
Advisor, Cyber Security Services
Dhirendra.kumar@kpmg.co.id

home.kpmg/id