

Judul : Data bill threatens 'exorbitant' fines
Tanggal : Senin, 12 September 2022
Surat Kabar : Jakarta Post
Halaman : 1

Data bill threatens 'exorbitant' fines

Draft legislation partly modeled on European Union's GDPR regulation

Deni Ghifari

The Jakarta Post/ Jakarta

Planned regulations aimed at strengthening data protection in Indonesia pose a significant threat to companies found to be non-compliant.

The private data protection (PDP) bill, which is currently awaiting final approval at the House of Representatives, stipulates fines of up to 2 percent of annual revenue for organizations guilty of exposing private information.

"Need to remind data controllers and processors to enforce proper encrypted security that can withstand cyberattacks, remembering that, if any violation happens, the fines will be quite high for corporations. They are exorbitant." Communications and Information Minister Johnny G. Plate said on Wednesday.

Administrative sanctions and criminal punishment will compel data controllers and processors to establish whole new data management systems to protect users' private details, a policy deemed novel in a country that has seen

several major data breaches over the past few years.

The ministry maintains that the fine of up to 2 percent of revenue is relatively forgiving given that the European Union's General Data Protection Regulation (EU GDPR) can entail fines of as much as 4 percent of a company's global annual revenue.

"In the past, data breaches just slipped through the cracks. Once this law is passed, that won't happen [any more], because it will be clear who is to be held accountable, up until what point and whether there will be criminal [proceedings] or administrative sanctions," said Abdul Kharis Mulyadhi, deputy chairman of House Commission I, which oversees intelligence and information.

The legal principles and norms in the bill—including criminal punishment—will apply as soon as the law is passed, but during a two-year period for companies to adjust the government can nullify administrative sanctions.

Having witnessed a similar transition in the EU, Martin Kohoutek, deputy executive direc-

tor of the German Indonesian Chamber of Industry and Commerce (EKOINDO), said two years was enough time to achieve compliance.

"However, I assume that the same thing will happen [in Indonesia] that happened in the European Union, namely [that] companies didn't move until the deadline came very close," said Kohoutek.

Furthermore, the majority of business players are skeptical about details of compliance such as private data processing termination, according to a survey conducted by the Indonesia Services Dialogue (ISD) Council, an industry association.

"Companies are willing to comply, but when it comes to actually meeting the requirements, this is where they need support and guidance. [...] Only around 23 percent are ready [to comply with] the deadline for terminating private data processing; the rest are not ready." ISD Council executive director Devi Ariyani told media representatives on Friday.

However hard it might be, Wa-

hyudi Djarot told *PusatKoran Post* that the law would set the underlying norms dictating how the industry is run, as the bill would turn into a benchmark of competitiveness based on consumers' trust.

"It will become the point of reference notwithstanding the challenges of implementation, and compliance, specifically considering how each company's capacity and resources are different," Wahyudi said.

Indonesia has been excluded from many international data transfers due to the absence of a data protection law, and this long-awaited bill can allow the country back into the community through international cooperation with nations that have equal data protection regulations.

Supporters of the bill say it will accomplish what the GDPR accomplished in the EU—the latter being the major reference for the conception of Indonesia's PDP bill.

"I definitely believe [that there is a direct correlation between such a law and improved data protection], because [a data breach prompting huge fines] goes through the press

like wildfire. This is not only relevant for big companies [...] it also affects smaller companies," Kohoutek said.

"They started to feel the pressure, so to speak [when the GDPR was enforced in the EU]. Many smaller companies were shaken, and they were like 'What do I actually have to do now?' I remember very vividly in 2018, a lot of companies were asking the chamber of commerce about what they have to do to comply with the law," he added.

Singapore is famous for stringent data protection rules enshrined in a law called the Personal Data Protection Act (PDPA).

"The PDPA provides a baseline standard of protection for personal data, complementing sector-specific legislative and regulatory frameworks, such as the Banking Act and the Insurance Act. It comprises various requirements governing the collection, use, disclosure and care of personal data in Singapore," said Pei Yuen Wong, chief technology officer at IBM Security Australia, Southeast Asia, New

Zealand and Korea.

"Apart from needing to ensure remediation, measures are being put in place to rectify the root causes of violations, e.g. improvements in processes, implementation of IT safeguards etc. A financial penalty is typically also imposed as a deterrence for future violations," he added.

Indonesia's PDP bill also orders the establishment of an overseeing agency, much like Singapore's Personal Data Protection Commission (PDPC). Wong explained that violations were published on the PDPC website as well as to show how seriously the country takes data protection.

"In general, the level of awareness among Singapore-based companies and the overall level of maturity in data protection measures taken by these companies have been observed to improve over time ever since the PDPA was put in place, especially after significant breaches and corresponding enforcement decisions were reported," Wong told the *Post* on Friday.