The approach to personal data protection in Indonesia amidst the global pandemic

DENTONS HPRP

April 15, 2020

Following the outbreak of COVID-19 and its development into a global pandemic, institutions and organizations in several countries have implemented exceptional measures to safeguard employees, customers, and other people from the far-reaching impact of the pandemic, one of which is by encouraging society to implement physical distancing. Although under extraordinary circumstances where physical distancing is a must in order to avoid the spread of COVID-19, institutions and organizations are endeavouring to maintain 'business-as-usual' and day-to-day activities of the society to the extent permitted by the local governmental institutions, under the pillars of public health and economic wellbeing.

Given the above circumstance, there have been significant changes as to how a person maintains ‘business-as-usual’ and day-to-day activities, including working and shopping, thus, resulting in the increase of the use of technology to accommodate the needs of society. Accordingly, we are all aware that the digital revolution has created new innovations that provide people with access to obtain, store and transmit real-time, broad, and complex data, including personal data.

With increasing levels of remote working, employees rely on applications or electronic systems to be able to accommodate their needs, which includes document storage, virtual meetings and/or conference calls. Furthermore, under the circumstance that physical distancing must be implemented, the public is transitioning to online shopping through applications or electronic systems provided by businesses to be able to meet their daily needs. It is essential to note that, in common practice, any person who utilizes electronic systems is generally required to register the use of the personal data of individuals.

Concurrently, the act of registering on an online platform or electronic system may expose risks that could adversely affect the privacy or confidentiality of a person's personal data. Furthermore, the increase in the use of technology will give rise to new challenges in protecting privacy and personal data, especially with the increased practice of personal data collection, utilization and dissemination through registration on and/or the utilization of online platforms or electronic systems that accommodate the needs of the public, such as for remote working or shopping.

The Ministry of Communication and Informatics (“**MoCI**”) Regulation No. 20 of 2016 concerning Protection of Personal Data in Electronic Systems (“**MoCI Reg. 20/2016**”) acts as the legal framework that significantly governs personal data in Indonesia, in that Article 1 point 1 jo. point 2 of MoCI Reg. 20/2016 defines personal data as every valid and factual information that is inherent and can be identified, whether directly or indirectly, with each individual.

An electronic system operator must be able to preserve, maintain, and safeguard the validity and protect the confidentiality of personal data that have been obtained, collected, processed, analyzed, stored, displayed, published, transmitted, disseminated, provided access to, and/or utilized, as personal data are essentially data that are confidential in nature which can only be obtained, collected, processed, analyzed, stored, displayed, published, transmitted, disseminated, provided access to, and/or utilized by virtue of a consent obtained from the owner of the personal data.

MoCI Reg. 20/2016 defines consent as a written statement, whether given manually and/or electronically, by the personal data owner after obtaining a complete explanation regarding the purpose and use of such personal data by the electronic system provider as well as the confidential or non-confidential nature of the personal data.

With the evolution of the digital era, personal data has become more vulnerable to misuse as a target for third parties to be able to obtain and collect data and/or information without authorized rights. For instance, some examples of data that can be categorized as personal data are information that can be used to identify a particular individual, such as an individual's full name, address, date of birth, identity card number, telephone number, kinship with family, and so forth. As an electronic system user and personal data owner, careful and conscientious consideration must be taken into account when providing data and/or information in an electronic system, particularly with regard to who will have access to it, for how long of a period, for what reason, whether the data and/or information can be modified by the electronic system provider, and so forth.

The law of personal data protection has developed along with the advancement of technology, information and communication. MoCI Reg. 20/2016, as the legal framework that significantly governs personal data in Indonesia, limits the acquisition and collection of personal data only to information that is relevant and in accordance with the purpose for which it was acquired and collected, which must be conducted accurately. Personal data that has been obtained and collected directly must be verified with the owner of the personal data or, if obtained indirectly, must be based on the results of various processed data sources that have a valid legal basis. The personal data can only be processed and analyzed as necessary in accordance with the needs of the electronic system provider that have been made known and agreed to by the personal data owner, where such agreement was obtained by the electronic system provider during the collection of data and/or information through a statement made by the personal data owner which expressly gives consent. However, further note that the processing or analysis of personal data that has been displayed or publicly announced by an electronic system for public services can be carried out without prior consent from the personal data owner.

With regard to the storage of personal data, an electronic system provider can only store personal data that has been verified for its accuracy in the form of encrypted data. Furthermore, in order to be able to display, announce, transmit, disseminate and/or provide access to personal data in an electronic system, an electronic system provider is required to:

a. obtain consent from the personal data owner; and
b. verify the accuracy and conformity with the purpose of obtaining and collecting the personal data.

Furthermore, when sharing personal data in an electronic system, the personal data owner is able to give consent to the electronic system provider regarding the confidential nature of their personal data, i.e. whether such data is confidential or not. In the event that the consent does not include consent for the disclosure of the confidential personal data, the electronic system provider and any person who obtains and collects such data, must maintain the confidentiality of the personal data without the need to obtain prior approval from the personal data owner.

MoCI Reg. 20/2016 also provides the obligation for electronic system providers to have an internal policy for obtaining, collecting, processing, analyzing, retaining, displaying, publishing, transmitting, disseminating, providing access to, and/or utilizing personal data as a form of preventative measure to safeguard and protect the personal data it manages. The preparation of such policy must consider aspects of the application of technology, human resources, methods, and costs and refer to applicable laws and regulations.

Inevitably, the expeditious development in the use of technology and the internet can have a negative impact on society, including the increase of cyber crime. The various forms of cyber crime relating to personal data can be in the form of theft of personal data, the distribution of personal data without authorized rights, and other crimes.

Pursuant to Article 36 of MoCI Reg. 20/2016, if a person were to obtain, collect, process, analyze, store, display,

publish, transmit, disseminate, provide access to, and/or utilize personal data, without authority or without compliance with the prevailing laws and regulations, such person will be subject to an administrative sanction in accordance with laws and regulations, in the form of the following:

a. verbal warning;
b. written warning;
c. suspension of activities; and/or
d. announcement on websites.

The administrative sanctions as mentioned above are imposed by MoCI or the head of the relevant supervisory agency and regulatory sector in accordance with laws and regulations.

In an effort to maintain 'business-as-usual' and day-to-day activities of the society under the special conditions in force, institutions and organizations have a business interest and legal obligation to preserve, maintain, and safeguard the privacy and confidentiality of personal data through organizational policies, contract terms, and statutory requirements on personal data protection. Such terms and policies are not to be exempted from its legality and validity and must stay in force, even as a result of adapting to the COVID-19 outbreak.

Although it is mandatory and essential for electronic system providers to preserve, maintain, and safeguard the confidentiality of an individual's personal data , there is still an urgency for personal data owners to be careful and conscientious in sharing their data and/or and information, in which personal risk assessments may be conducted to balance out a personal data owner's duties of care along with their interests, whether business or in general, in order to ensure and maintain business resilience and day-to-day continuity of activities amidst the global pandemic.

For further information related to the services provided, please contact the Partner listed under key contact.

The article above was prepared by Erwin Kurnia Winenda (Partner), **Mika Isac Kriyasa** (Senior Associate), and **Inaya Safa Nadira** (Associate).

Your Key Contacts

Erwin Kurnia Winenda
Partner, Jakarta
D +62 21 5701837
M +62 812 90732284
erwin.winenda@dentons.com