DENTONS HPRP

Grow | Protect | Operate | Finance

Certification for Personal Data Processing

Prepared by:
Mika Isac Kriyasa (Partner) and Cattelya Nabila Mediarman (Associate)

The development of information technology and digitalization requires more practical and detailed protection in its implementation, as it facilitates convenient access for business actors to connect with consumers, which also makes it easier for business actors to obtain consumers' personal data.

Regulations on personal data aim to, among other things, protect and guarantee the basic rights of citizens in relation to their personal protection, and to ensure that the public gets good services from corporations, public agencies, international organizations, and governments regarding the processing of their personal data.

Personal Data, as defined in Law Number 27 of 2022 on Personal Data Protection ("**Indonesian PDP Law**"), means data which separately or in combination with other information, either directly or indirectly through an electronic or non-electronic system, identify or make it possible to identify individuals. The Indonesian PDP Law's transitional provisions state that upon the Indonesian PDP Law coming into effect, all provisions of laws and regulations that regulate personal data protection remain valid insofar as they do not conflict with the provisions of the Indonesian PDP Law.

Processing of Personal Data

Article 16 of the Indonesian PDP Law provides that processing of personal data includes:

a. acquisition and collection;

b. filtering and analysis;

c. storage;

d. fixes and updates;

e. display, announcement, transfer, dissemination, or disclosure; and/or

f. deletion or destruction,

of personal data. Aside from the foregoing, Article 4 of Ministry of Communications and Informatics Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems, as one of the implementing regulations on the personal data protection law in Indonesia, provides that the electronic systems that are used for processing personal data via the types of processing stated in the Indonesian PDP Law referred to above must be certified, the implementation of which certification process should be in accordance with the provisions of laws and regulations.

Certification for Electronic Systems which Process Personal Data

The certification for electronic systems which process personal data is further explained in Ministry of Communications and Informatics ("**MOCI**") Regulation Number 4 of 2016 on Information Security Management Systems ("**MOCI Reg 4/2016**"), and National Cyber and Crypto Agency ("**NCCA**") Regulation Number 8 of 2020 on Security Systems in the Implementation of Electronic Systems ("**NCCA Reg 8/2020**").

To address the question of why the provisions on electronic system security are issued by 2 (two) different institutions, it is worth noting that the NCCA was established as a fusion of 2 (two) institutions: (i) the National Crypto Agency and Directorate of Information Security, and (ii) the Directorate General of Information Application (Aptika) of MOCI. Therefore, in this article, we will discuss the certification for electronic system under the 2 (two) laws and regulations.

Article 4 of MOCI Reg 4/2016 and Article 6 of NCCA Reg 8/2020 simultaneously regulate the classification of electronic systems based on the risk approach, namely:

a. **Strategic Electronic System**, or an electronic system which has serious impact on the public interest, public services, the smooth running of the state, or state defense and security;
b. **High Level Electronic System**, an electronic system whose impact is limited to sectoral and/or certain regional interests; and
c. **Low Level Electronic System**, an electronic system that is not included in points a and b above.

Further, the standardization set out for each classification of electronic system is provided in Article 9 of NCCA Reg 8/2020, as follows:

a. **for Strategic Electronic Systems**, the electronic system must implement SNI ISO/IEC 27001, other safety standards related to cyber security set by the NCCA, and other safety standards related to cyber security set by the Ministry or Institution;
b. **for High Level Electronic Systems**, the electronic system must implement SNI ISO/IEC 27001 and/or other safety standards related to cyber security set by the NCCA, and other safety standards related to cyber security set by the Ministry or Institution; and
c. **for Low Level Electronic Systems**, the electronic system must implement SNI ISO/IEC 27001, or other safety standards related to cyber security set by the NCCA.

Pursuant to the above, the differences between the standardization for each classification of electronic system above arise from the different sources of standards given for the implementation (i.e., (a) the system has to comply with SNI ISO/IEC 27001, NCCA, and the Ministry's standard, (b) the system can only comply with the standards given by SNI ISO/IEC 27001 or with the standards given by the NCCA or both sets of standards, and in either case with the standards from the Ministry, and (c) the system is not required to comply with the standards given by the Ministry).

In addition to the foregoing, after classifying the electronic systems based on their risk approach, the electronic system must also have a certification of Information Security Management System ("**ISMS**") which comes from a certification institution that is recognised by the MOCI and NCCA, and will be valid for a maximum of 3 (three) years from the date of its issuance.

How to Obtain the Certification

Under Article 16 of MOCI Reg 4/2016 and Article 29 of NCCA Reg 8/2020, in order to obtain the ISMS certification, the electronic system operator must first implement SNI ISO/IEC 27001.

SNI ISO/IEC 27001 is a standardization for ISMS set forth by the National Standardization Agency, which describes the guidelines and requirements for creating, implementing, managing risks, and maintaining and documenting an ISMS. SNI ISO/IEC 27001 is also an adaptation of the widely recognized ISO/IEC 27001.

After the operator implements SNI ISO/IEC 27001 and complies with the obligations for the relevant classification of the electronic system set out in Article 9 of NCCA Reg 8/2020 above, the certification agency will assign an Information Security Auditor to conduct an ISMS audit of the electronic system operator, and the auditor will report to the certification agency on the audit results. In the event the electronic system operator has met the standards set out by the institutions, then the ISMS certificate will be issued.

Sanctions for Not Obtaining the Certification and Complying with the Standardization

As the law requires every electronic system operator to obtain an ISMS certification, those who do not obtain the certification then will be liable to an administrative sanction in the form of (i) a written warning, and (ii) temporary suspension of the electronic system's Indonesian Domain Name, as provided in Article 25 of MOCI Reg 4/2016.

Further, NCCA Reg 8/2020 also provides for sanctions that can be imposed on parties who do not implement on their electronic systems SNI ISO/IEC 27001 and other standardizations given by the NCCA or the Ministry, which sanctions take the form of a written warning given after the violation is discovered.

Conclusion

To conclude, an electronic system which processes personal data must be certified under the ISMS certification which is required under MOCI and NCCA regulations. In order to obtain the ISMS certification, the electronic system operator must also implement SNI ISO/IEC 27001 as the widely recognizable national standard for ISMS.

We, Dentons HPRP, provide full-range services for our clients including offering counsel, advice, and guidance on regulatory compliance, and we would be happy to assist you to implement the SNI ISO/IEC 27001 and obtain the ISMS certification from the institution.

-o0o-