ASIAN BUSINESS LAW INSTITUTE

FUTURE OF PRIVACY FORUM

ABLI-FPF CONVERGENCE SERIES

Indonesia

Status of Consent for Processing Personal Data

JULY 2022

AUTHORED BY

Dominic Paulger

Policy Manager (APAC), Future of Privacy Forum

PROJECT LEAD

Dr. Clarisse Girot

Honorary Senior Fellow, Asian Business Law Institute

CONTRIBUTORS

Danny Kobrata

Partner, K&K Advocates

Bhredpita Socarana

Senior Associate, K&K Advocates

ACKNOWLEDGEMENTS

This Report benefitted contributions and editing support from Elizabeth Santhosh and Catherine Shen.

TABLE OF CONTENTS

1. INTRODUCTION

This report summarizes the roles played by consent and related provisions, including alternatives to consent, in Indonesia's data protection framework and highlights provisions which can serve as indicators for convergence of laws and regulations in this area across Asia Pacific.

Indonesia currently has no comprehensive data protection law. However, several sectoral laws and regulations (collectively, the "**PDP Regulations**") provide for personal data protection in electronic systems. These include:

- Law No. 11 of 2008 on Electronic Information and Transactions[1] (as amended by Law No. 19 of 2016[2]) ("**Law 11/2008**");
- Ministry of Communication and Information Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("**MCI 20/2016**")[3]; and
- Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("**GR 71/2019**"),[4] which supplements Law 11/2008 with additional provisions to, among others, ensure recognition and respect for the rights and freedoms of persons[5] (note that GR 71/2019 has not yet been implemented).

Broadly, the PDP Regulations impose specific requirements on collection and processing of personal data by electronic system operators ("**ESOs**"), i.e., any person, state administrator, business entity or society that provides, manages, and/or operates an "electronic system."[6]

Note that a first-of-its-kind Personal Data Protection Bill ("**PDP Bill**") was introduced in Indonesia's Parliament on January 28, 2020. The current draft of this bill provides several legal bases for processing of personal data, including, but not limited to, consent. However, note that the PDP Bill has not yet been passed, and the draft legislation remains subject to change.

2. CONSENT AND PRIVACY SELF-MANAGEMENT IN EXISTING LAWS AND REGULATIONS

The PDP Regulations rely heavily on consent as a mechanism for privacy self-management. Consent serves as the primary or default justification for processing personal data under the PDP Regulations,[7] including for cross-border data transfers, subject to certain exceptions and derogations. As the PDP Regulations do not recognize implied or inferred consent, express consent is typically required.

Relevant authorities have not provided any specific explanation as to the underlying policy motivations for consent requirements in the PDP Regulations. However, the prevalence of consent requirements

---

[1] Available in Indonesian at https://jdih.kominfo.go.id/produk_hukum/view/id/167/t/undangundang+nomor+11+tahun+2008+tanggal+21+april++2008

[2] Available in Indonesian at https://jdih.kominfo.go.id/produk_hukum/view/id/555/t/undangundang+nomor+19+tahun+2016+tanggal+25+november+2016

[3] Available in Indonesian at https://jdih.kominfo.go.id/produk_hukum/view/id/553/t/peraturan+menteri+komunikasi+dan+informatika+nomor+20+tahun+2016+tanggal+1+desember+2016

[4] Available in Indonesian at https://jdih.kominfo.go.id/produk_hukum/view/id/695/t/peraturan+pemerintah+nomor+71+tahun+2019+tanggal+10+oktober+2019

[5] Explanation of Government Regulation of the Republic of Indonesia Number 71 of 2019 on Implementation of Electronic Systems and Transactions, page 1.

[6] Law 11/2008, Articles 1(6)(a) and 1(1); MCI 20/2016, Articles 1(6) and 2; GR 71/2019, Article 1(4). Note that an "**electronic system**" is defined as a series of electronic devices and procedures that function, prepare, collect, process, analyze, store, display, announce, transmit, and/or disseminate electronic information (Law 11/2008, Article 1(5); MCI 20/2016, Article 1(5); GR 71/2019, Article 1(1) – see also Articles 1(8) and 1(30)).

[7] Law 11/2008, Article 26(1); MCI 20/2016, Article 2(2)(c); GR 71/2019, Article 14(3).

appears to be based on notions of control over processing of personal data, which in turn appear to be based on the view that personal data protection is one aspect of a broader right to privacy.

2.1. Law 11/2008

Law 11/2008 establishes consent as the default legal basis for use, via electronic media, of any information that contains personal data.[8] This provision is subject to any exceptions provided by other laws or regulations.[9]

2.2. MCI 20/2016

MCI 20/2016 requires consent for:

- initial collection of personal data, unless laws and regulations provide another applicable legal basis;[10]
- processing or analysis of personal data,[11] unless the data is publicly available;[12]
- disclosure of personal data to a third party;[13] and
- use of personal data by a third party to whom the personal data has been disclosed.[14]

2.3. GR 71/2019

A key principle under GR 71/2019 is that personal data should be collected in a limited, specific, lawful, and fair manner, with the knowledge and consent of the "**personal data owner**" (i.e., data subject).[15]

Article 14(3) of GR 71/2019 establishes consent as a valid legal basis for collecting and processing personal data.[16] Article 14(4) of GR 71/2019 *may* also provide alternative legal bases for processing of personal data without the need to obtain consent, where processing is for fulfillment of:

- an obligation under a contract to which the personal data owner is a party;[17]
- a personal data controller's obligation under applicable laws and regulations;[18]
- a vital interest of the personal data owner;[19]
- the personal data controller's authority pursuant to applicable laws and regulations;[20]
- the personal data controller's obligation to provide public services for the public interest;[21] and/or
- other legitimate interests of the personal data controller and/or personal data owner.[22]

However, the drafting of Article 14(4) of GR 71/2019 is ambiguous as it requires that the processing of personal data must be justified under any of the above conditions *in addition to* consent pursuant to Article 14(3) of GR 71/2019 (emphasis added). This gives rise to an alternative interpretation that the provisions of Article 14(4) impose additional requirements that apply on top of a separate requirement

---

[8] Law 11/2008, Article 26(1).
[9] Law 11/2008, Article 26(1).
[10] MCI 20/2016, Article 9(1).
[11] MCI 20/2016, Article 12.
[12] MCI 20/2016, Article 13.
[13] MCI 20/2016, Article 9(2). If the personal data owner does not provide consent, then the data must be kept confidential. However, even if the personal data owner consents to disclosure of his/her personal data, the data must be kept confidential if this is required by applicable laws and regulations (MCI 20/2016, Article 9(3).
[14] MCI 20/2016, Article 24.
[15] GR 71/2019, Article 14(1)(a).
[16] GR 71/2019, Article 14(3).
[17] GR 71/2019, Article 14(4)(a).
[18] GR 71/2019, Article 14(4)(b).
[19] GR 71/2019, Article 14(4)(c).
[20] GR 71/2019, Article 14(4)(d).
[21] GR 71/2019, Article 14(4)(e).
[22] GR 71/2019, Article 14(4)(f).

to obtain consent. This interpretation would be consistent with the principle in Article 14(1)(a) of GR 71/2019 that consent of personal data owners is required for collection and processing of personal data.

2.4. Sectoral regulations

Under sectoral laws and regulations, consent is usually required for collection and processing of personal data, except where processing of personal data is required by other applicable laws and regulations (e.g., disclosure of personal data for government supervision purposes).

a. Health sector

Law No. 36 of 2009 on Health ("**Law 36/2009**")[23] and Ministry of Health Regulation No. 269/Menkes/Per/III/2008 of 2008 on Medical Records ("**MoH 269/2008**")[24] regulate all activities by doctors/dentists, health professionals, and health service facilities in relation to patients' medical records. Any disclosure of information relating to a patient's identity, diagnosis, medical history, examination history, and medication history is only permitted if made pursuant to a request of the patient's request or with the patient's consent to such disclosure.

With regard to health research, Law 36/2009 and MoH 269/2008 both require the data subject's written consent where the data subject's personal data and/or medical records are to be used for the purpose of health research.

Further, the National Health Research and Development Ethics Committee, an independent commission established by the Ministry of Health, has issued Guidelines and Standards on Ethics for National for Health Research and Development ("**Health Research Ethics Guidelines**")[25] which apply to any activities relating to health research.

Broadly, the Health Research Ethics Guidelines requires health researchers to protect and keep confidential any information obtained from an individual or a group of individuals, even where the health research is in the public interest. Informed consent of data subjects is required before the data subjects to participate in health research: the data subjects must be provided with clear information on the purpose, method, and risks of the research, and the possible research outcomes, including any possible negative impact on them from the research. Consent to participate in health research is considered valid only in respect of research purposes which have been notified to the data subject. If any information or samples provided by the data subject are to be used for any purpose other than the research purpose notified to the data subject, then informed consent must be obtained afresh for this new purpose.

Where researchers require access to the data subjects' medical records, and any of the information sought is capable of identifying the data subject (including where anonymized data can be deanonymized through connection with other information), researchers must obtain the data subject's consent.

Where a data subject cannot provide informed consent due to health factors (e.g., physical or mental disability) or because the data subject is deceased, consent may be obtained from the data subject's biological relatives, but the data itself may not be disclosed to them.

b. Financial sector

Several laws apply in the financial sector.

---

[23] Available in Indonesian at https://jdih.setneg.go.id/viewpdfperaturan/UU%20Nomor%2036%20Tahun%202009.pdf

[24] Available in Indonesian at https://pelayanan.jakarta.go.id/download/regulasi/peraturan-meneteri-kesehatan-nomor-269-tentang-rekam-medis.pdf

[25] Available in Indonesian at https://keppkn.kemkes.go.id/2022/01/26/pedoman-dan-standar-etik-penelitian-dan-pengembangan-kesehatan-nasional/

In banking services, Law No. 7 of 1992 on Banking, as amended by Law No. 10 of 1998,[26] Financial Service Authority ("**FSA**") Regulation No. 6/POJK.07/2022 on the Consumer Protection in Financial Services Sector ("**FSA 6/2022**"),[27] and Central Bank of Indonesia Regulation No. 22/20/PBI/2020 on Protection of Indonesian Bank Consumers,[28] prohibit "financial services businesses" ("**FSBs**")—which include banks, insurance providers, and peer-to-peer lenders—from providing and/or disclosing consumer information to any third party, unless the FSBs obtain written consent from consumers, or disclosure is required by applicable laws and regulations.

Additionally, FSA Regulation No. 77/POJK.01/2016 on Technology-Based Fund-Lending Services[29] requires peer-to-peer lenders to obtain consent for collection and processing of personal data and ensure the confidentiality and integrity of personal data, transactional data, and/or financial data from the time that such data is collected until it is erased.

"Payment services providers" (e.g., electronic wallet, electronic money, payment transaction providers), ("**PSPs**") are also required to protect the confidentiality and security of consumers' data. A PSP is prohibited from providing and/or disclosing information regarding its consumers to any third party unless the PSP has obtained written consent from the consumer or unless applicable laws and regulations require provision and/or disclosure of the data.

3. CONSENT AND PRIVACY SELF-MANAGEMENT IN THE DRAFT PERSONAL DATA PROTECTION BILL ("PDP BILL")

The current draft of the PDP Bill provides several equivalent legal bases for processing of personal data, in a format similar to that of Article 6 of the GDPR. These include consent[30] or one of six alternative bases,[31] which apply where processing is:

- necessary:
  - for the performance of a contract to which the data subject is a party;[32]
  - to fulfill a request of the data subject prior to entering into a contract;[33]
  - to comply with a statutory obligation to which the data controller is subject;[34]
- to protect the vital interests of the data subject;[35]
- in exercise of the data controller's authority under applicable laws and regulations;[36]
- to fulfill the data controller's obligation to provide services in the public interest;[37] or

---

[26] An English translation is available at https://www.ojk.go.id/en/kanal/perbankan/regulasi/undang-undang/Pages/Act-of-the-Republic-of-Indonesia-Number-7-of-1992-concerning-Banking-as-Amended-by-Act-Number-10-of-1998.aspx

[27] Available in Indonesian at https://www.ojk.go.id/id/regulasi/Documents/Pages/Perlindungan-Konsumen-dan-Masyarakat-di-Sektor-Jasa-Keuangan/POJK%206%20-%2007%20-%202022.pdf

[28] Available in Indonesian at https://www.bi.go.id/id/publikasi/peraturan/Pages/PBI_222020.aspx

[29] Available in Indonesian at https://www.ojk.go.id/id/regulasi/otoritas-jasa-keuangan/peraturan-ojk/Documents/Pages/POJK-Nomor-77-POJK.01-2016/SAL%20-%20POJK%20Fintech.pdf

[30] PDP Bill, Article 18(1).

[31] PDP Bill, Article 18(2). These legal bases are discussed in further detail under "COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT SUBJECT TO A RISK IMPACT ASSESSMENT" and "COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT IN OTHER CIRCUMSTANCES DEFINED BY LAW" below.

[32] PDP Bill, Article 18(2)(a).

[33] PDP Bill, Article 18(2)(a).

[34] PDP Bill, Article 18(2)(b).

[35] PDP Bill, Article 18(2)(c).

[36] PDP Bill, Article 18(2)(d).

[37] PDP Bill, Article 18(2)(e).

- to fulfill other legitimate interests, after balancing the data controller's and data subject's respective interests.[38]

However, note that since the PDP Bill has not yet been enacted, these provisions are still subject to change.

4. CONDITIONS FOR CONSENT

4.1. Definition and forms of consent

a. PDP Regulations

Law 11/2008 neither defines consent nor elaborates on the forms that valid consent may take.

By contrast, MCI 20/2016 defines consent as a declaration of approval given by the personal data owner after receiving a full explanation of the purpose of processing and of the confidentiality status and accuracy of the data.[39] This definition appears to require an affirmative action on the part of the personal data owner.

Under MCI 20/2016, an ESO is required to obtain written consent from the data subject before collecting and processing personal data. The consent should be obtained using a form that is in the Indonesian language and that provides information on the purpose and objective of data collection. The consent can be obtained manually or electronically.[40]

Under GR 71/2019 and MCI 20/2016, consent must be given explicitly and may not be obtained through concealment of information, mistake, negligence, or coercion.[41]

b. PDP Bill

Under the PDP Bill, consent may take the form of a recorded written or oral agreement[42] to one or more specific purposes communicated to the personal data owner.[43]

4.2. Withdrawal of consent

a. PDP Regulations

Data subjects have a right to withdraw their consent. Where a data subject withdraws consent, the ESO must erase the data subject's personal data pursuant to the data subject's right to erasure.

b. PDP Bill

In the event that a personal data owner withdraws consent to processing of his/her personal data, the data controller must cease any processing of that data[44] no later than 72 hours after receiving the withdrawal[45] and erase and/or destroy the personal data. However, the PDP Bill expressly provides that erased personal data may be recovered if the data controller receives a written request to that effect from the data subject.[46]

---

[38] PDP Bill, Article 18(2)(f).
[39] MCI 20/2016, Article 2(4).
[40] MCI 20/2016, Article 6.
[41] Explanation of Government Regulation of the Republic of Indonesia Number 71 of 2019 on Implementation of Electronic Systems and Transactions, page 6.
[42] PDP Bill, Article 19(1).
[43] PDP Bill, Article 18(1).
[44] PDP Bill, Articles 25(1) and 38(1)(b).
[45] PDP Bill, Article 25(2).
[46] PDP Bill, Article 38(3).

4.3. Bundled consent

Indonesian laws and regulations do not recognize bundled consent.

5. CONSENT FOR SPECIAL CATEGORIES OR USES OF DATA

MCI 5/2020 distinguishes two categories of personal data, namely:

- "specific personal data," which comprises:
  - medical information and data;
  - genetic data;
  - data as to a person's sexual orientation;
  - personal data of minors;
  - personal financial data; and
  - other data specified by law; and
- "non-specific personal data" (i.e., data other than specific personal data).

However, the purpose behind this two-tiered categorization is unclear because there seems to be no difference in how MCI 5/2020 treats the two categories of personal data. It. Therefore appears that the general rules on consent would apply to both specific and non-specific personal data.

5.1. Children

Pursuant to MCI 20/2016, where consent is required for processing of a minor's personal data, the consent must be obtained from the minor's parents or legal guardian.[47]

However, the specific age range within which a person will be considered a minor for this purpose is unclear as MCI 20/2016 does not specify such an age range and although there are several Indonesian laws that regulate the age of majority of a person, the age limit varies from one regulation to the next. For example, under Indonesia's Civil Code, the age to perform a legal action, such as entering a contract, is 21 years old or the age at which a person legally marries. By contrast, Law No. 23 of 2002 on Child Protection, as amended by Law No. 35 of 2014 ("**Law 23/2002**"), defines a child as anyone who is below the age of 18 years.

It is not yet clear which age will be used for classification of minors when Indonesia passes comprehensive personal data protection law.

6. CONSENT FOR CROSS-BORDER DATA TRANSFERS

6.1. PDP Regulations

Generally, an ESO may transfer personal data out of Indonesia after obtaining the data subject's consent and verifying the accuracy of the personal data.

6.2. PDP Bill

The current draft of the PDP Bill establishes consent as one of several legal bases for the cross-border transfer of personal data.[48] Other bases include:

[47] MC 20/2016, Article 37.
[48] PDP Bill, Article 49(1)(d).

- where the destination jurisdiction provides an equivalent or higher level of protection of personal data to that provided by the PDP Bill;[49]
- where transfer is pursuant to an international agreement;[50] or
- where there is a contract between data controllers which stipulates a standard that is in line with the PDP Bill and/or guarantees protection as stipulated under the PDP Bill.[51]

7. TRANSPARENCY AND NOTICE

7.1. PDP Regulations

GR 71/2019 requires ESOs who request consent for processing of personal data to convey the purpose(s) of processing to the personal data owner.[52]

The PDP Regulations stipulate that consent for collection of personal data must be obtained by providing a form written in the Indonesian language explaining the purpose of the processing (e.g., storage, service provision, etc.).

Consent is only valid if the data subject has received a full explanation of the purpose for collecting personal data and any activities that will be conducted in relation to the personal data. This information may be conveyed to the data subject in the form of a privacy notice or privacy policy, which must be written clearly in a manner that is easily accessible by the data subjects and in the Indonesian language. There is, however, no express provision stipulating the degree of specificity to which the purpose for collection of personal data should be described.

7.2. PDP Bill

For consent to be deemed valid under the PDP Bill, the data subject must be provided with the following information:

- the legality of personal data processing;[53]
- the purpose of personal data processing;[54]
- the type and relevance of the personal data to be processed;[55]
- the retention period of personal data;[56]
- details regarding any personal data collected;[57]
- the period during which personal data will be processed;[58] and
- the rights of the personal data owner under the PDP Bill.[59]

8. SANCTIONS AND ENFORCEMENT

Failure to comply with obligations in relation personal data is subject to administrative sanctions as stipulated under MCI 20/2016, including:

[49] PDP Bill, Article 49(1)(a).
[50] PDP Bill, Article 49(1)(b).
[51] PDP Bill, Article 49(1)(c).
[52] GR 71/2019, Article 14(3).
[53] PDP Bill, Article 24(1)(a).
[54] PDP Bill, Article 24(1)(b).
[55] PDP Bill, Article 24(1)(c).
[56] PDP Bill, Article 24(1)(d).
[57] PDP Bill, Article 24(1)(e).
[58] PDP Bill, Article 24(1)(f).
[59] PDP Bill, Article 24(1)(g).

- a verbal warning;[60]
- a written warning;[61]
- suspension of business activities;[62] and/or
- publication of a notice on the website of the Ministry of Communication and Information Technology ("**MCI**").[63]

There is currently no specific authority in Indonesia that is responsible for enforcing privacy and personal data protection. The closest equivalent appears to the MCI, which has the authority to impose sanctions for non-compliance. It is understood that the MCI has previously commenced investigations against companies that have failed to comply with personal data protection principles and has issued sanctions, mostly in the form of written warnings. However, this approach may change as the MCI, in coordination with Ministry of Finance, is in the process of preparing a Government Regulation Draft on Non-Tax State Revenue that would govern imposition of administrative fines under GR 71/2019 and in turn enable the government to impose fines against companies that fail to comply with data protection obligations.

At the sectoral level, the FSA actively enforces personal data and/or privacy requirements in the financial sector and has engaged in enforcement actions against peer-to-peer lenders which operate without obtaining licenses from the FSA and illegitimately process personal data.[64]

Further, under Law 11/2008, a data subject whose rights under this provision are infringed may lodge a claim for damages against the infringing party.[65]

9. COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT SUBJECT TO A RISK IMPACT ASSESSMENT

As discussed above, GR 71/2019 appears to provide for alternative legal bases to process personal data without the need for consent, including "fulfillment of other legitimate interests of the personal data controller and/or personal data owner."

However, the relevant provisions are vaguely drafted, and it is expected that the PDP Bill, once enacted, will resolve this ambiguity. Specifically, the current draft of the PDP Bill clearly provides that personal data may be processed without consent where processing is for the fulfillment of a legitimate interest, taking into account the goals and needs of the data controller, the balance between the interests of the data controller, and the rights of the personal data owner.[66]

The PDP Bill's "legitimate interests" provision appears to be based on the similarly worded Article 6(1)(f) of the GDPR. However, unlike its equivalent in the GDPR, the PDP Bill provision does not specify *whose* interests may be taken into account and *how* the balancing exercise should be conducted. By contrast, Article 6(1)(f) of the GDPR specifies that a data controller may rely on its own interests or those of a third party, that processing of personal data on this basis must be necessary for pursuit of such interests, and that such processing is permitted only where the interests relied upon are not overridden by the rights and freedoms of the data subject.

It is also expected that the PDP Bill, once enacted, will require data protection officers to undertake impact assessments under certain conditions.

However, since the PDP Bill is still being discussed in Parliament as of the date of this report, there is no clear indication of whether or how such provisions will be implemented.

---

[60] MCI 20/2016, Article 36(1)(a).
[61] MCI 20/2016, Article 36(1)(b).
[62] MCI 20/2016, Article 36(1)(c).
[63] MCI 20/2016, Article 36(1)(d).
[64] "Fintech stakeholders declare war on illegal P2P lenders" *The Jakarta Post* (13 December 2018), available at https://www.thejakartapost.com/news/2018/12/13/fintech-stakeholders-declare-war-on-illegal-p2p-lenders.html
[65] Law 11/2008, Article 26(2).
[66] PDP Bill, Article 18(2)(f).

10. COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT IN OTHER CIRCUMSTANCES DEFINED BY LAW

10.1. PDP Regulations

Generally, the PDP Regulations permit ESOs to collect and process personal data only with the explicit consent of the data subject and only recognize exceptions to this requirement for purposes of:

- supervision by relevant ministries and/or institutions; or
- investigations by law enforcement.

In this regard, an ESO which receives a written request from a relevant authority may disclose personal data to that authority and provide the authority with access to the ESO's electronic system and/or electronic data (including personal data) without the data subjects' consent.

In other circumstances (including where personal data is publicly available), general provisions on consent would still apply, and an ESO would still be required to obtain valid consent from the relevant data subject in order to process the data.

As discussed above, GR 71/2019 appears to provide for alternative legal bases to process personal data without the need for consent, namely:

- fulfillment of contractual obligation if the data subject is one of the parties;
- fulfillment of a legal obligation to which the personal data controller is subject, pursuant to applicable laws and regulations;
- fulfillment of a vital interest of the data subject;
- implementation of the personal data controller's authority pursuant to applicable laws and regulations;
- fulfillment of the personal data controller's obligation to public services for public interest; and/or
- fulfillment of other legitimate interests of the personal data controller and/or personal data owner.

However, the relevant provisions are vaguely drafted, and it is expected that the PDP Bill, once enacted, will resolve this ambiguity.

Indonesia's civil law system rarely relies on a rule of interpretation as a formalized way of interpreting legal provisions. Authorities interpret provisions of law in the context of the broader law in which the provisions are located.

However, the general approach to interpreting exceptions in law or the absence of law on a given topic is that if there is no specific provision regulating a certain practice, then that practice would not generally be prohibited. Another point to note is that in the absence of regulation or if a regulation is unclear, Law No. 30 of 2014 of Government Administration grants relevant authorities the right to exercise discretion to fill in gaps in regulations. Government institutions in Indonesia have consistently adopted this approach, particularly in relation to personal data protection issues.

10.2. PDP Bill

The current draft of the PDP Bill permits processing of personal data without the data subject's consent where processing is:

- necessary:
    - for the performance of a contract to which the data subject is a party;[67]

[67] PDP Bill, Article 18(2)(a).

  - to fulfill a request of the data subject prior to entering into a contract;[68]
  - to comply with a statutory obligation to which the data controller is subject;[69]
- to protect the vital interests of the data subject;[70]
- in exercise of the data controller's authority under applicable laws and regulations;[71]
- to fulfill the data controller's obligation to provide services in the public interest;[72] or
- to fulfill other legitimate interests, after balancing the data controller's and data subject's respective interests.[73]

10.3. COVID-19

During the COVID-19 crisis, personal information has been processed in accordance with the Infectious Disease Control and Prevention Act as necessary to contain the spread of infections. Though emergency regulations were issued in response to COVID-19, there have also been no specific rules exempting the implementation of certain laws.

MCI Decree No. 171 of 2020 on the Declaration of the use of the *Pedulilindungi* Application to Conduct Medical Surveillance for Coronavirus Disease 2019 (COVID-19) Treatment,[74] as amended by MCI Decree No. 253 of 2020[75] ("**MCI Decree**") provides for use of contact-tracing applications. This Decree refers to various laws (including Law No. 24 of 2007 on Disaster Management and Law No. 36 of 2009 on Health) which—in principle—allow the Government to perform certain actions to address certain health situations. The MCI Decree also clarifies that collection or processing of personal data by the developer of a contact-tracing application must be made in accordance with the law.

There have been no meaningful discussions or developments on the Government's personal data protection policies in its response to COVID-19, despite the fact that there have been personal data breaches during the course of the pandemic.

---

[68] PDP Bill, Article 18(2)(a).
[69] PDP Bill, Article 18(2)(b).
[70] PDP Bill, Article 18(2)(c).
[71] PDP Bill, Article 18(2)(d).
[72] PDP Bill, Article 18(2)(e).
[73] PDP Bill, Article 18(2)(f).
[74] Available in Indonesian at https://jdih.kominfo.go.id/produk_hukum/view/id/735/t/keputusan+menteri+komunikasi+dan+informatika+nomor+171+tahun+2020
[75] Available in Indonesian at https://jdih.kominfo.go.id/produk_hukum/view/id/780/t/keputusan+menteri+komunikasi+dan+informatika+nomor+253+tahun+2020

ASIAN BUSINESS LAW INSTITUTE

The Asian Business Law Institute (ABLI) is a permanent think tank based in Singapore that initiates, conducts and facilitates research with a view to providing practical guidance in the field of Asian legal development and promoting the convergence of Asian business laws.

1 SUPREME COURT LANE | LEVEL 6 | SINGAPORE 178879 ABLI.ASIA | INFO@ABLI.ASIA

FUTURE OF PRIVACY FORUM

The Future of Privacy Forum (FPF) is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Learn more about FPF by visiting fpf.org.

1350 EYE STREET NW | SUITE 350 | WASHINGTON DC 20005 FPF.ORG | INFO@FPF.ORG