PRIVACY INTERNATIONAL

Submission on Indonesia's Draft Law on the Protection of Personal Data, 2018

August 2018

About us

This submission is made by Privacy International (PI).

Privacy International was founded in 1990. It is the leading charity promoting the right to privacy across the world. Working internationally through an International Network of partners, Privacy International works, within its range of programmes, investigates how our personal data is generated and exploited and advocates for legal, policy and technological safeguards. It is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised, and reported to, among others, the Council of Europe, the European Parliament, the Organisation for Economic Co-operation and Development, and the United Nations.

To find out more about privacy and data protection in Indonesia, please refer to 'The State of Privacy in Indonesia' (last updated in February 2018).

Contacts

Ailidh Callander
Legal Officer, Privacy International
ailidh@privacyinternational.org

Alexandrine Pirlot de Corbion
Programme Lead, Privacy International
alex@privacyinternational.org

Overview

Privacy is a fundamental human right. Protecting privacy in the modern era is essential to effective and good democratic governance. This is why data protection laws exist in over 120 countries worldwide including 25 African countries,[1]and instruments have been introduced by international and regional institutions such as the African Union,[2] the OECD,[3] Council of Europe,[4] and ECOWAS.[5]

We welcome the effort by the Government of Indonesia to reaffirm its commitment to rights of individuals by regulating the processing of their personal data through the adoption of a Data Protection Act.

However, the Data Protection Bill proposed has a number of significant shortcomings. We recommend that to effectively protect privacy and to meet international standards in protecting personal data, that full consideration be given to the areas of concern and improvements outlined below under each Part of the Bill.

[1] See Graham Greenleaf, Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey (2017) 145 Privacy Laws & Business International Report, 10-13, UNSW Law Research Paper No. 45available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2993035

[2] See the African Union Convention on Cyber security and Data Protection, 2014, available at http://pages.au.int/infosoc/cybersecurity

[3] 3See the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, updated in 2013, available at http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[4] See the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108, 1981, available at http://conventions.coe.int/Treaty/en/Treaties/html/108.htm

[5] See the Supplementary Act on personal data protection within ECOWAS, February 2010, at http://www.ecowas.int/publications/en/actes_add_telecoms/SIGNED-Personal_Data.pdf

Chapter I – General Provisions

Article 1

‘**personal data’** we welcome the recognition in the definition that it includes data from which an individual is both directly and indirectly identifiable. However, the understanding of what personal data encompasses could be strengthened by linking to Article 5 of the Bill which include a non-exhaustive list of personal data

‘owner of personal data’
Article 1 (6) defines what an ‘owner of personal data’ of personal data is but it is unclear to whom this term actually refers. Is this term referring to the data subject, i.e. the person whose personal data it is or is it the Controller of Personal Data i.e. the organisation managing the processing of Personal Data.

‘**processing’**
The definition of ‘processing’ provided for in Article 1 (10) is unclear and is also limited to activities undertaken by the data processor. Strongly suggest revising adoption of a more comprehensive definition to cover the entire ‘lifecycle’ of data - from its creation to its deletion - as well as the use of data to reveal other data. This definition should also be linked to Article 24 of the Bill which includes a non-exhaustive list of what processing includes.

Article 2

This provision outlines the principles on the basis of which the law is executed. However, the list provided fails to provide for widely-recognised data protection principles including:

- **Fairness and transparency**: Personal data must be processed in a fair and transparent manner. This principle is key to addressing practices such as the selling and/or transfer of personal data that is fraudulently obtained. ‘Fairness and transparency’ are essential for ensuring that people’s data is not used in ways they would not expect.
- **Lawfulness**: Personal data must be processed in accordance with the law, this includes both compliance with existing laws, e.g. human rights obligations and also the requirement that there be a legal basis for the data processing, as stipulated in data protection law.
- **Accountability:** An entity which processes personal data, in their capacity as data controllers or processors, should be accountable for complying with standards, and taking measure which give effect to the provisions provided for in a data protection law. Those with responsibility for data processing must be able to demonstrate *how* they comply with data protection legislation, including the principles, their obligations, and the rights of individuals.

Furthermore, we would like to flag to the following in relation to the current list provided for in Article 2.

The list fails to clearly explain what the principles are, and thus this article should be strengthened to provide further details. Without this clarity, the meaning and importance of the principles is unclear – in particular in relation to the last two.

Article 2(h) refers to “fitness of purpose”. This use of the term ‘fitness’ is slightly unclear. The aim of this principle should be about ensuring that all personal data be collected for a determined, specific, and legitimate purpose. Any further processing must not be incompatible with the purposes specified at the outset (i.e. the point of collection). This essentially means that it is not acceptable to state that

you need a person's data for one purpose, and then use it for something else without notice or justification.

Article 2(i) refers to the right to destroy or delete. We question what is meant by this? Without any further explanation this is confusing as a principle. Is it meant to mirror the requirement that personal data not be retained longer than necessary (if so, is this not covered by the retention principle?), or is it meant to reflect an individual's right to erasure? Furthermore what is the intended difference between destroy and delete? If this principle is to remain in the Bill, further clarity must be provided.

Article 4

The scope outlined in Article 4 is confusing. Further clarity needs to be provided in order to ensure it is clear to whom the law applies.

Legislators have an obligation to protect the rights of those in their jurisdiction, including the right to privacy and data protection. Therefore, in order that individuals are not deprived of the protections they are entitled to, data protection frameworks should be clear as to how the law applies and protects individuals in each of these scenarios:

- The data controller/data processor is established in the relevant jurisdiction, even if processing takes place elsewhere;
- The controller or processor is not established within that jurisdiction, but is processing personal data of an individual in that jurisdiction; and
- The data is transferred to a third party outside that jurisdiction.

Chapter II – Types of Personal Data

Article 5

This Article should be linked together with the definition of personal data provided in Article 1. Personal data is any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier. It is helpful to provide this non-exhaustive list but whether or not it is Personal Data should not be restricted to whether unauthorised disclosure can harm the person's right to privacy. It should be enough that the person is identifiable, directly or indirectly, from the data. Furthermore, the list – even though non-exhaustive – should go further and include other types of data including online identifiers. Otherwise this clause could have the opposite effect and lead to the view that personal data is limited to the listed identifiers.

Article 6

We are unfamiliar with the terms used "generic nature" and "specific nature" provided in Article 6. Based on Article 6 (3) we can presume that personal data of "specific nature" refers to what is commonly known as sensitive personal data or special categories of data.

It is important that emphasis be given to the fact that this sort of data, here referred to as personal data of "specific nature" are sensitive and/or special, and therefore attract higher safeguards, including limitations on the permitted grounds for processing it.

A glaring omission from this definition is data about an individual's race or ethnicity, as well as their philosophical beliefs and membership of a trade union.

Furthermore, some consideration should be given as to whether there are any other categories specific to the Indonesian context that should be added. Considering the local context and realities is an important step in ensuring that relevant safeguards are provided for in legislation.

It is not clear how Article 6(3)(k), will work in practice, who will be empowered to designate personal data of a 'specific nature'?

It is also important that higher protections extend to data which *reveals* sensitive personal data, through profiling and the use of proxy information (for example, using someone's purchase history to infer a health condition), it is possible for those processing data to infer, derive and predict sensitive personal data without actually having been explicitly provided with the sensitive personal data.

Chapter III – Controller of Personal Data

Part Two

Article 8

Article 8 notes that the management, or processing, of personal data must be based on "approval" of the owner of personal data, i.e. the data subject. We would like to receive clarity that the term "approval" used in this article and thereafter refers to "consent".

Furthermore, we are concerned by the broad exemptions to obtain "approval", i.e. consent, from an individual to process their personal data. The wording of each of the exemptions are extremely vague and broad, furthermore there is no qualification that the processing be necessary or that the failure to rely on an exemption would cause prejudice/ harm. Each of these exemptions should be re-examined and narrowed. Exemptions for these purposes outlined in Article 8(2) should only be applied when strictly necessary and proportionate, and not been seen as a blanket exemption.

Article 8 specifically refers to "personal data of a specific nature", clarity is needed on what basis "personal data of a generic nature" may be processed.

Article 9

Consent is not defined in the Bill, this is problematic throughout but specifically in relation to special information.

The Bill needs to defined consent as *"freely given", "specific", "informed"* and "*unambiguous*", and elaborate on definition and conditions of '*consent'* in relation to the collection and processing of "personal data of specific nature", i.e. sensitive personal data.
Whilst, it is standard that consent not be the only condition/ legal basis for processing personal data – the exceptions should be clear and narrow (as noted above in relation to Article 8(2). Therefore, the provisions of Article 9(3) should be similarly narrow regarding legal provisions, agreements with the Owner of personal data and threats to the data subject. The wording of the current provisions is too vague.

In relation to the information to be provided to the individual as outlined in Article 9 (2), we would suggest the following to be considered and included:

- information as to the identity of the controller (and contact details);
- the recipients of the personal data;
- whether the controller intends to transfer personal data to a third country and the level of protection provided;
- the existence of the rights of the data subject;
- the right to lodge a complaint with the supervisory authority;
- the existence of profiling, including the legal basis, the significance and the envisaged consequence of such processing for the data subject;
- the existence of automated decision-making and at the very least meaningful information about the logic involved, the significance and the envisaged consequence of such processing for the data subject;
- the source of the personal data (if not obtained from the data subject);
- whether providing the data is obligatory or voluntary; and
- the consequences of failing to provide the data.

Furthermore, it is important to emphasise that this information must be provided at the time of collection and be provided for in a manner that is user-friendly and accessible to the individual.

Article 9 specifically refers back to Article 8 which covers "personal data of a specific nature", clarity is needed on the obligations associated with the processing of "personal data of a generic nature".

Article 10

We welcome the right provided to individuals to withdraw consent. In relation to this provision, we would suggest including the need for the data controller to take positive action to confirm with the individual that their request has been processed, their consent withdrawn, and their data deleted. It should be as easy to withdraw consent/ 'approval' as it is to provide it.

Article 17

We welcome the obligation placed on data controllers to provide a right of access to individuals. However, the current wording of this provision is limited.

It is not clear why the history of the management of the Personal Data is limited to a one year period, an individual should have the right to request access to <u>all</u> of their personal data.

The law should provide minimum requirements, including for the process of obtaining data relating to those requirements. These include requirements on:

- *Timeframe:* this should be within a reasonable and stated time.
- *Cost:* individuals should bear no cost for obtaining information about processing and a copy of their personal data.
- *Format*: the information provided to the data subject should be in a form that is readily intelligible to them and does not require them to have any particular expertise or knowledge in order to comprehend the information they are provided with.
- *Information*: Together with access and a copy of the Personal Data, the individual should have the right to specific information about the processing of their personal data – this should be similar to the types of information provide pre-processing (Article 9) and cover the processing taken to date.

- *Explanation and appeal*: if the request is denied, the data subject has a right to be given reasons why, and to be able to challenge such denial. Furthermore, if their challenge is successful they must have the right to have the data erased, rectified, completed or amended.
- *Clarity*: if there are to be any exemptions to this right these should be clearly set out in law and their application explained to the data subject.

Exemptions for these purposes outlined in Article 17(3) should only be applied when strictly necessary and proportionate, and not been seen as a blanket exemption.

Article 21

We welcome the obligation placed on data controllers to notify individuals of data breaches. However, we would encourage re-wording this provision so that the obligation to notify does not depend on the need for a "harm" to have occurred which seems to be what is currently implied.

Furthermore, this obligation should be clearly stipulated in law and provide:

- Clarity on the time period, which must require notification to occur as soon as possible after the controller/processor is made aware of the breach;
- A requirement to notify whenever there is a risk to the rights of the individuals concerned, and
- What information should accompany the breach notification, such as the nature of the breach, those who are affected, the likely consequences, and the measures taken to address the breach and mitigate adverse effects.

There should also be an obligation to notify the Commission of a breach.

Article 23

The obligation to destroy and delete links into the principle of not retaining data longer than necessary and appears to be an expression of the right to erasure under Article 23(2)(d). In order to ensure that this right is effective, the timescale in which the request must be responded to must be included. There should also be a clear safeguard to the extent that the right could interfere with the right to freedom of expression and information.

Chapter IV – Processing of Personal Data

Article 24

This Article should be linked with the definition of personal data at the beginning of the Bill.

Article 25

The exemption to providing information in Article 25(3) should be limited, it should only be relied upon to the extent that the application of the exemption is necessary as providing the information would prejudice the investigation.

Chapter V – Rights of the Owner of Personal Data

Part One – General

We welcome the inclusion of the current rights under Part One of Chapter V. However, there are several rights missing for the current Bill including, which we would urge be added including:

The right to object: An individual has the right to object to their data being processed at any point. If the individual objects, the onus must be on the data controller to provide evidence for the need to continue processing the data of that individual, with reasons which override the interests, rights, and freedoms of that individual. Certain rights to object should be absolute, such as in relation to direct marketing.

The right to data portability: This is a right that is increasingly included in data protection frameworks around the world. This give the right to data subjects to request that personal data about themselves that is processed by the data controller be made available to them in a universally machine-readable format, and to have it transmitted to another service with the specific consent of that individual. This can be particularly useful in the context of certain types of processing to allow individuals to receive their data and have it transferred in an interoperable format – enabling people to switch between services more easily. This right is a step towards ensuring that the data subject is placed in a central position and has a full power over his or her personal data.

The rights in relation to profiling and automated decision-making: A data protection law should provide effective protection and rights in relation to both profiling and automated decision-making. This should include all of the above rights and those already provided for in the Bill being applied in the context of profiling and automated decision making to address specific concerns related to these ways of processing personal data. These rights do not need to be dealt with together as this can lead to unnecessary confusion. However, it is important that both are covered in a data protection framework.

- **Profiling:** Profiling, just as any form of data processing also needs a legal basis. The law should require that organisations who profile are transparent about it and individuals must be informed about its existence. Individuals must also be informed of inferences about sensitive preferences and characteristics, including when derived from data which is not per se sensitive. Since misidentification, misclassification and misjudgement are an inevitable risk associated to profiling, controllers should also notify the data subject about these risks and their rights, including to access, rectification and deletion. Individual's rights need to be applied to derived, inferred and predicted data, to the extent that they qualify as personal data. The Bill should also include a definition of profiling.

- **Automated decision making:** This Bill should impose restrictions and safeguards on the ways in which data can be used to make decisions. Individuals should have a right not be subject to purely automated decision-making. The law may provide for certain exemptions, i.e. as when it is based on a law (e.g. fraud prevention), or when the individual has given their explicit consent. However, any such exemptions must be limited, as well as and clearly and narrowly defined. Even where exemptions allow for automated-decision making, an individual should have the right to obtain human intervention, to receive an explanation of the decision and be able to challenge it.

Article 26

We would recommend that this right outline in more detail the information to be provided by the data controller to the individual as well the timeframe and form in which the information is provided so that is corresponds to the obligation of the data controller provided for in Article 17 of the Bill.

Article 27

It is unclear what is mean here by allowing the individual "the right of completing" their personal data. Further clarity is sought in this regard.

Article 28

As noted in relation to other rights in the Bill, the timescale for a Controller responding to such a request should be set out on the face of the Bill. Together with the requirement to provide confirmation once the data has been corrected.

Article 29

To align itself with the obligation provided for in Article 10 and Article 23, we would suggest including the need for the individual to be given evidence that their request has been processed, and their data deleted. There should also be safeguards for the right to freedom of expression and information.

Article 30

We welcome the inclusion of a provision to enable an individual to bring a lawsuit and to receive compensation for damages. The Bill should be clear that individuals may seek compensation for material and non-material damages, i.e. individuals should be able to seek compensation for distress as well as, for example, financial damage.

The Bill should also facilitate collective redress both so that individuals can appoint NGOs to act on their behalf and that NGOs may take action against those that violate data protection law, without the need for a mandate from individuals.

Part Two - Exceptions to the Protection of Personal Data

Article 32

The exemptions provided for in this provision are too broad and are open to abuse. It is essential to ensure that, where it provides for such exceptions, the law also provides in-depth details on the specific circumstances in which the rights of data subjects can be limited. These provisions should be limited, necessary and proportionate, and be clear and accessible to the data subject. Moreover, these should not be blanket exceptions but must only pertain to certain rights in very specific and limited situations and be clearly set out by the law.

Failure to properly define and limit these exceptions will undermine public trust in data protection.

Most data protection frameworks include an exemption for household processing. This should be included and made clear at the beginning in terms of the scope of the Bill.

Chapter VI – Transfer of Personal Data

Article 33

This provision seems to indicate that only two requirements must be met to transfer the data to a third partly, namely approval from the individual and complying, i.e. consent, and respecting the objective, i.e. the purpose limitation. Important to consider other grounds for processing which may be called upon and to regulate those clearly.

Article 35

One of the provisions permitting transfers of personal data outside the Republic of Indonesia is where the country has a level of protection equal to that set out in the Bill. Further details should be provided of how this assessment is to be made in practice. For example, are the Commission going to undertake adequacy assessments of other frameworks and if so under which criteria?

Chapter VII – Direct Marketing

Article 37

Consideration should be given as to whether it would be helpful to define Direct Marketing. Furthermore, a timescale for such a request should be provided and it should be made clear what type of 'reprimand' the Commission may take.

Chapter VII – Establishment of a Code of Conduct of Controller of Personal Data

Article 38

The establishment of a Code of Conduct by industry must not undermine the provisions in the law (the principles, the obligations and the rights). The Code of Conduct should be subject to consultation with civil society (this should be clear in Article 38(2)(c) and approval by the Commission.

Chapter XI – Commission

Article 42

Clarity needs to be provided on the process and the timeframe within which the Commission would be set-up as well as any decision-making on the appointment of its members, and the resources allocated to the Commission to fulfil its mandate.

The Commission's powers should be clearer on the face of the Bill, including their ability to investigate both in response to a complaint and proactively and also their ability to enforce the law and the tools and powers with which to do that.

Consideration should be given to giving the Commission the necessary powers and resources to carry out their own investigation so that they do not, for example, have to rely on law enforcement as suggested in Article 42(3)(b).

It is also not clear from this provision what action the Commission would then take if they have decided and determined that there has been a violation of Personal Data.

Article 43

It is not clear what the process for Commission Regulations will be. This should be specified so that wide delegated powers are not provided to the Executive without sufficient parliamentary scrutiny. Any such regulations, made under delegated powers in the Bill, must be consulted upon and made public.

Chapter XIII – Administrative Sanctions

Article 53

The proposed fines are considerably lower than the fines provided in similar legislation in other contexts, for example in the EU – where the maximum fine is €20 million or 4% of global annual turnover. Whilst the law should be sensitive to the regulatory environment in Indonesia it is important that a lower possible financial penalty is less of a deterrent to violating the law. Consideration could be given as to whether to introduce a maximum fine based on turnover of a company and whether there should be tiered fines depending on the nature of the violation.

Chapter XV – Transitional Provisions

Article 56

Whilst transitional provisions are standard with many legislative changes, we consider the period of 1 year too long.