PUBLIC CONSULTATION PAPER NO. 01/2020

REVIEW OF PERSONAL DATA PROTECTION ACT 2010 (ACT 709)

Start Date : 14 February 2020

End Date : 28 February 2020

PUBLIC CONSULTATION PAPER NO. 01/2020
REVIEW OF PERSONAL DATA PROTECTION ACT 2010 (ACT 709)

INTRODUCTION

Personal Data Protection Act 2010 (Act 709) which was enacted in 2010 serves the purpose to regulate personal data processing in the commercial transactions. After almost 10 years of operation, there are needs to further strengthen the enforcement and implementation of Act 709, taking into consideration the emerging issues on personal data protection impacting both data users and data subjects from the aspects of economic, social and technology. In recent years, there have been growing cases of data breaches involving the multi-type of data users from different sectors which leads to challenges in implementing and enforcing the personal data protection law.

Therefore, the study to review Act 709 has been conducted in 2019 with the aim to focus on the effective implementation of Act 709 compared to other data protection laws internationally and to explore areas for improvements. The study saw the engagement of experts from the industries, regulators, government agencies and academicians in series of lab to bring forth and discuss the improvement ideas to strengthen the Act 709.

PUBLIC CONSULTATION PAPER

In the process of reviewing the act, Personal Data Protection Commissioner (PDP Commissioner) seeks to gauge the views and comments of the public through this public consultation paper. Feedbacks and comments should not be limited to the issues stated in the 'Points to be Considered' in each proposed item under Part I (1-22), as it only serve as guidance. Further to the views and comments, the suggestion can also state whether there is a need for a new provision, amendments to the as-is provisions, amendments to the regulations, or code of practice or issuance of guidelines.

SUBMISSION OF COMMENTS

Individuals/parties that interested to participate in this public consultation may do so by:

i) Write your comment/feedback (concise and with justification) in Microsoft Word format, concerning a specific number of the paragraph and page number (if appropriate) of the proposal in Part I;

ii) Fill in your particulars in Part II;
iii) **Email no. i) and ii) to pcpdp@pdp.gov.my no later than Friday, 28th February 2020**.

PARTICIPATION

This public consultation is open to anyone who has the interest to get involved in the process of the Act 709 review. **All submission should reach the Commissioner by 28th February 2020**. Please do not hesitate to contact afiza@pdp.gov.my or noreen@pdp.gov.my if you have any enquiry.

Thank you very much for your interest and participation.

Personal Data Protection Commissioner
Ministry of Communications and Multimedia Malaysia

PART I – PROPOSED IMPROVEMENT SUGGESTION

1) Data processor to have a direct obligation under Act 709

- There is no clear provision that gives direct obligation to a data processor to comply with Act 709.
- Under the Security Principle [s9(2)], a data user must ensure that any data processor appointed will protect personal data from any loss, misuse, modification, unauthorized disclosure, etc.
- There are many cases of data breaches involving data processors. Hence, the proposed direct obligation to Act 709 will prevent the risk of data breach incident among the data processors.
- Therefore, the PDP Commissioner is considering to directly regulate data processor.
- Points to be considered:
    i. Data processor to have direct obligation under Act 709 and to be registered with the PDP Commissioner.
    ii. The definition of data processor to include data processor appointed by the Federal Government and State Governments.

2) The right to data portability

- Data portability is a concept that gives individuals the right to obtain and reuse their data for other purposes across different services. It is the right for a data subject to get access to his data in a structured, machine-readable format which can be transferred from one data user to another to get services.
- This concept supports the free flow of personal data transaction and it has been applied in many countries such as the Philippines [s18, Data Privacy Act 2012], dan European Union (EU) [Art. 20, GDPR].
- However, the implementation of this concept in Malaysia has to be studied further so that it will not spur the rise of a data breach incident.
- The Commissioner is considering to insert a new provision on the right to data portability.
- Points to be considered:
    i. The proposed approach of the right data portability.
    ii. Impact of this right is being implemented in Malaysia.

3) Data user to appoint a Data Protection Officer

- Currently, there is no provision in the Act which mentions the obligation of a data user to appoint Data Protection Officer (DPO). In a normal situation, a compliance officer in an organisation will take charge of the personal data protection matters.
- DPO is responsible to oversee data protection strategy and implementation in an organisation which enable to increase the level of compliance with Act 709.
- GDPR [Art.37] and Singapore [s11(3)] have described concisely in their law about the appointment of DPO.
- PDP Commissioner is considering to add a new provision in Act 709 to make it obligatory for a data user to appoint a DPO, and to issue a guideline on the mechanism of having a DPO.
- Points to be considered:
    i. The proposed requirement to appoint a DPO.
    ii. The elements to be considered in the guidelines on DPO (ie. categories of data users that must appoint DPO, based on size of data user or amount of data held).

4) Data user to report data breach incident to the Commissioner

- There is no provision in the Act to instruct a data user to report the incident of a data breach to PDP Commissioner.
- The PDP Commissioner however, has proactively taken the initiative to issue a Data Breach Notification (DBN) form to data user involved. The information in the DBN form is essential for the PDP Commissioner to make assessment and decision on the incident.
- However, the DBN form issued by the PDP Commissioner cannot be made compulsory to data user as there is no specific provision in the Act.
- EU-GDPR [Art.33], Philippines [s20(f)] dan North Korea [Art.34] have clearly described in their law on data user obligation to inform the Commissioner on data breach incident.
- PDP Commissioner is considering to add a new provision to make it mandatory for a data user to report on data breach incident, and to issue a guideline on the mechanism of data breach incident reporting.
- Points to be considered:
    i. The proposed mandatory DBN.
    ii. The impact of having all data user to report about the data breach incident in their organisation.
    iii. The elements to be considered in the guideline on data breach incident reporting.

5) Clarity in the consent of data subject

- General Principle [s6] has clearly stipulated consent of data subject.
- Personal Data Protection Regulations 2013 [P.U.(A)335] also has mentioned that consent must be recorded and maintained. For sensitive personal data, a data user must obtain explicit consent from the data subject before any personal data can be processed further.
- However, consent in the General Principle is combined with some other topic such as the processing purposes and the collection of excessive personal data.
- There are countries which have a specific provision on consent. EU-GDPR [Art.37] and Singapore [s43] for instance describe only consent in a specific provision.
- PDP Commissioner is considering to restructure s6 as to add clarity on the consent subject matter. The focus will be in the scope and application of consent through the personal data life cycle.
- Points to be considered:
    i. What is your opinion on the proposed restructuring and the idea of adding clarity to data subject's consent?
    ii. What is your view if consent should be in one specific provision?
    iii. What is your view on the impact of having a default consent?

6) Transfer of personal data to places outside Malaysia

- Clear provision and condition of transferring personal data to places outside Malaysia are essential to facilitate e-commerce transactions and free trade agreements.
- The current provision in s129 stated that a data user shall not transfer any personal data of a data subject to a place outside Malaysia unless to such place specified by the Minister - [s129(2)] a whitelist.
- Whitelist seems to curb and set as a barrier for a data user to transfer personal data to places outside Malaysia. Ever since the Act was enacted, there is no whitelist been issued and gazetted by the Minister.
- PDP Commissioner is considering to restructure the provision and to remove the issuance of whitelist in s129.
- Points to be considered:
    i. The proposed whitelist to be removed from this Act.
    ii. The impact of removing the whitelist from s129.

7) Data user to implement privacy by design

- Privacy by design is a concept that integrates privacy into the system life cycle built by the data user.
- At the moment, there is no specific provision to instruct a data user to consider privacy by design in the whole process of developing a manual or digital system in an organisation.
- The application of privacy by design is emerging as a method of proactive security measures by a data user to reduce the risks of data breaches.
- PDP Commissioner is considering to instruct any new system to apply privacy by design and to issue a guideline on the mechanism.
- Points to be considered:
    i. The proposed implementation of privacy by design to a data user.
    ii. The impact if privacy by design is a mandatory provision to all data user.
    iii. The elements to be considered in preparing the privacy by design's guideline.

8) Data user to establish Do Not Call Registry

- Do Not Call Registry (DNCR) is a service which allows data subject to opt-out from receiving unsolicited direct marketing[1] materials.
- This concept is significant as it helps to strike a balance between the needs of industry and the right of an individual. In this agile world, some data user needs to engage with direct marketing as a way to continue to thrive in businesses while a data subject will need some space of privacy such as not to be contacted for marketing purposes at any time by the data user.
- DNCR seems like an early initiative for a data user to protect data subject's personal data from being processed excessively and without consent.
- Singapore for instance, has a clear provision on DNCR - [Part IX PDPA 2012] Do Not Call Register.
- PDP Commissioner is considering to insert a new provision of DNCR.
- Points to be considered:
    i. The proposed DNCR is to be established by each data user.
    ii. The impact of having DNCR in Malaysia.

[1] Direct marketing means the communication by whatever means of any advertising or marketing material which is directed to particular individuals.

9) Right of data subject to know the third party which his personal data has been/to be disclosed to

- A data subject has the right to access his personal data held by a data user [s12].
- For data user, a disclosure list registry to the third party is a compulsory [no. 5, P.U.(A)335] and need to be shown whenever required by the authorized officers of the PDP Commissioner's office during the inspection of personal data system [s101]. Other than that, a data user is also obliged to impose the class of third party disclosure in a written notice (privacy/PDP notice or statement).
- GDPR [Art.15(c)] is giving the right of access to the data subject which includes the recipients or categories of recipient to whom the personal data have been or will be disclosed.
- PDP Commissioner is considering to extend the right of data subject to know specifically his personal data has been disclosed to which third party.
- Points to be considered:
  i. The proposed right of data subject to know the third party which his personal data has been/to be disclosed to.
  ii. The important elements to be considered in the implementation and enforcement of such right.

10) Civil litigation against data user

- Act 709 is a part of cyber law that has been endorsed during the implementation of the Multimedia Super Corridor (MSC).
- There is no such provision in the Act that mentions of a data subject right to take civil litigation against a data user. Nevertheless, an aggrieved data subject can still pursue civil litigation under the common law.
- In countries like Singapore [s32(1)], North Korea [Art. 57], Macau [Art. 14] and EU-GDPR (Art. 82], there is a provision which clearly provides the civil litigation that can be taken by a data subject against a data user.
- Points to be considered:
  i. The proposed specific provision to stipulate the civil litigation that can be pursued by a data subject against a data user.

11) Address privacy issue arising from data collection endpoints

- Technologies and techniques are employed in processing personal data in commercial activities. The use of technology encompasses the entire aspect of an individual's life. In the new era where digital technology and e-commerce revolution occur at any situation surmount the need to process personal data adequately, with high-security assurance.
- As a result, many techniques such as facial recognition and smart trackers are widely being used by data user as data collection endpoints to collect data and to identify an individual for many purposes.
- PDP Commissioner is considering to issue a clear policy regarding the endpoint security which use the technology like encryption to dwindle the risks of a data breach incident.
- Points to be considered:
    i. Technological advancement and personal data protection.
    ii. Other technologies that may contribute to the vulnerability of personal data protection.
    iii. The important elements to be considered in preparing the endpoint security policy.

12) The application of Act 709 to the Federal Government and State Governments

- Act 709 is currently not applicable to the Federal Government and State Governments. Only the statutory bodies need to comply with this Act.
- A massive study is needed if the Act is to be extended to the Federal Government and State Governments.
- There are numerous existing laws and regulations (for example, the Official Secrets Act 1972) that govern those parties.
- PDP Commissioner is considering to issue a guideline to statutory bodies to clarify the agency's compliance with Act 709.
- Points to be considered:
    i. Act 709 is extended to the Federal Government and State Governments.
    iii. The impact if the Federal Government and State Governments are exempted from compliance with the provision of Act 709.

13) The exchange of personal data for data user with an entity located outside Malaysia

- Data users that have branches operating overseas need to exchange information with the entity at some point.
- In general, Act 709 does not preclude the transfer of personal data abroad if it complies with the requirements [s129]. However, security measures should be implemented to curb data breach incident to occur during the transfer.
- PDP Commissioner is considering to issue a guideline on the mechanism and implementation of cross border data transfer.
- Points to be considered:
    i. The important things to be considered in the cross border data transfer's guideline.

14) Exemption of business contact information from compliance with Act 709

- Business contact information such as the business card or name card shows personal data such as name, telephone number and designation. Business contact information is widely used across many sectors and activities.
- Despite it facilitate communications, yet there are risks of data user misusing the business card information for inappropriate purposes.
- Singapore however, exempt the business contact information from compliance with it's PDPA 2012 [s5].
- PDP Commissioner is considering to issue a guideline to clarify the status of business contact information.
- Points to be considered:
    i. The usage of business contact information.
    ii. The impact if business contact information is exempted from compliance with Act 709.
    iii. The elements to be considered in preparing the guideline for the usage of business contact information.

15) Disclosure of personal data to government regulatory agency

- The data user is allowed to disclose personal data for other than the purpose consented at the collection time, which meant for prevention of crime [s39(b)(i)], investigation or authorised and required by law, or by court order [s39(b)(ii)].
- However, despite the authorization stipulated in a certain Act, there are times where data users reluctant to disclose personal data under their possession to a government regulator.

- PDP Commissioner is considering to issue a guideline to add clarification and help data users to understand the level of disclosure to government regulatory agencies.
- Points to be considered:
    i. The elements to be considered in preparing the guidance of personal data disclosure to government regulatory agencies.

16) Class of data user based on business activity

- To date, there are 13 classes of data users which are required to register with PDP Commissioner. These data users are classified based on sectoral and the law that governs the respective industries.
- Data user which do not belong to the 13 classes of data users are not required to register but still have to comply with Act 709.
- Points to be considered:
    i. The proposed classes of data users based on business activities.
    ii. The impact specifically in compliance if data users are classified according to business activities such as health and beauty and food and beverages.

17) Voluntary registration

- As of now, there are 13 classes of data users that are mandatory to register with the PDP Commissioner.
- There is no current provision that allows data users from other than 13 classes of data users to register with the PDP Commissioner.
- Compared to the UK, starting 25th May 2018, all data users in the UK are obliged to register with the Commissioner and to pay personal data protection fee [Data Protection (Charges and Information) Regulations 2018].
- Points to be considered:
    i. Voluntary registration by data users that do not belong to the 13 classes of data users.
    ii. The impact if all data users in Malaysia are required to register with the PDP Commissioner.

18) The application of Act 709 to non-commercial activity

- This Act only regulates the processing of personal data in commercial transactions.
- A non-commercial transaction such as charities and religious activities are not governed by this Act.
- As a comparison, Canada is also applying its data protection to only commercial transaction whereas, in the Philippines, Japan, North Korea and EU, data protection act regulates both commercial and non-commercial transactions.
- Points to be considered:
    i. The proposed extension of the Act to non-commercial transactions.
    ii. The impact if Act 709 applies to non-commercial transactions.

19) The application of Act 709 to data users outside Malaysia which monitor Malaysian data subject

- It is stipulated in s3(2) that Act 709 does not apply to personal data processed outside Malaysia unless it is intended to be processed further in Malaysia.
- The fact that Malaysia is embracing on the expension of digital economy, it is inevitable to avoid the processing of personal data outside of Malaysia. Hence, it is impossible to hinder the activity of surveillance and profiling of Malaysian citizen overseas.
- EU-GDPR [Art.22 (1)] stated the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
- Points to be considered:
    i. The proposed application of Act 709's to data users outside Malaysia who monitor and do profiling of Malaysian data subject.

20) Data users to provide a clear mechanism on the way to unsubscribe from online service

- A data subject can withdraw consent to process personal data [s38] while s43 allows a data subject to prevent the processing of personal data for direct marketing purposes.
- As current provisions provide enough rights for data subjects to withdraw the processing of personal data for services, the PDP Commissioner is considering to issue a guideline to data user on the mechanism of digital and electronic marketing.

- Points to be considered:
    i. The proposed data user to provide a clear mechanism for data subject to unsubscribe from online service.
    ii. The important elements to be considered in preparing the guideline of processing personal data in the digital and electronic marketing.

21) Data users are allowed to make first direct marketing call

- s43 provide the right to data subject to prevent the processing of personal data for direct marketing purposes. A data subject may do so by giving written notice to data user to stop calling for direct marketing.
- PDP Commissioner is considering to issue a guideline on the implementation of direct marketing for data users.
- Points to be considered:
    i. The proposed data user to make the first direct marketing call to the data subject.
    ii. Your views on the 'opt-out' method.
    iii. The important elements to be considered in preparing the direct marketing guideline.

22) The processing of personal data in cloud computing

- Cloud computing as storage is popular due to its flexibility, efficiency, and cost-effectiveness.
- Despite the benefits, data breach incidents happen within the environment of clouds.
- As of now, there is no specific provision in the Act that stated a direct regulation on the cloud service providers.
- Some views cloud service provider as a data processor as it keeps personal data in the platform. But others view cloud service provider not as a data processor as it only provides infrastructures to the storage of personal data.
- Regardless, a cloud service provider cannot be exempted from the obligation of protecting personal data under its purview.
- PDP Commissioner is considering to issue a guideline on usage of cloud computing for data users.
- Points to be considered:
    i. Your views on the cloud services provider.
    ii. The impact if there no contractual clauses on personal data protection between data user and its appointed cloud service provider.
    iii. The scope of guideline about the usage of cloud computing.

PART II – ABOUT YOU

i) Name:

ii) Email address:

iii) You are commenting as:
(please mark ✓ in the third column given)

No.	Respondent category	✓
1	**Data subject** (individuals who are the subject of the personal data)	
2	**Registered data user** (data user which belong to the 13 classes of data users)	
3	**Unregistered data user** (any person that process personal data but does not belongs to the 13 classes of data users)	
4	**Data processor** (any person that process data solely on behalf of the data user)	

iv) If you provide comments as **no. 2, 3 or 4**, please state your organisation's name:

v) If you provide comments as **no. 2**, please state your data user's sector (from the 13 classes of data user):

vi) If you provide comments as **no. 3 or 4**, please state your organisation business's sector: