**PUBLIC CONSULTATION PAPER NO.1/2015**

**THE PROPOSED STANDARDS FOR PERSONAL DATA PROTECTION**

1. **PURPOSE**

Public Consultation Paper No.1/2015 aims to obtain feedback from data users and data subjects in relation to the understanding of personal data protection. To make the Personal Data Protection Standards 2015 as a reference document, Personal Data Protection Commissioner (the Commissioner) has agreed to merge three standards, namely Security Standards, Storage Standards and Data Integrity Standards into a consistent document. This step is in in line with the requirements of the Regulations of Data Protection 2013, Personal Data Protection Act 2010.

In this regard, the feedback received through this public consultation paper will be analysed and the results will be used in the preparation of the final draft of the standard. The final draft will be presented to the 11 classes of data users before being registered by the Commissioner.

1. **BACKGROUND**

Since January 2015, Personal Data Protection Commissioner's Office has been carrying out monitoring visits on the premises of the registered data users. As a result of the visit, various feedback and findings are collected to be used as input to develop the minimum standards.

In order to make the standard sufficient to regulate data users in Malaysia, the Commissioner has worked together with the Department of standards Malaysia and CyberSecurity Malaysia as well as taking into account the views of experts and also the best practices at the international level.

In addition, the Special Committee at the Department of Personal Data Protection, headed by the Deputy Commissioner has implemented several stages of evaluation before PUBLIC CONSULTATION PAPER No. 1/2015 is published.

1. **INSTRUCTIONS TO DATA USERS AND DATA SUBJECTS**

Data users and data subjects are required to:-

1. Read carefully the contents of the Public Consultation Paper No. 1/2015
2. Write your feedback in Appendix A
3. Send your feedback to:

**KERTAS KONSULTANSI AWAM BIL. 1/2015**

**Aras 6, Kompleks KKMM, Lot 4G9,**

**Jabatan Perlindungan Data Peribadi**

**Kementerian Komunikasi dan Multimedia Malaysia**

**Persiaran Perdana, Presint 4,**

**Pusat Pentadbiran Kerajaan Persekutuan,**

**62100 Putrajaya.**

1. The Public Consultation Paper No. 1/2015 can also be sent **via e-mail: mastura@pdp.gov.my or by fax: 603-89117959**
2. The deadline for sending your feedback is on **27 July 2015 (Monday)**
3. **ACKNOWLEDGEMENT**

The Department of Personal Data Protection (JPDP) and the Commissioner acknowledge and thank you for the feedback submitted.

**(MAZMALEK MOHAMAD)**

**Personal Data Protection Commissioner**

**Appendix A:**

*PUBLIC CONSULTATION PAPER No. 1/2015*

**PART 1- GENERAL INFORMATION**

1. **Entities : Data User/Data Subject/Issuer of Industrial License**
2. **Industry : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**
3. **Contact number/E-mail (optional): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**PART 2 - FEEDBACK**

1. **APPLICATION**

|  |  |
| --- | --- |
| ***No.*** | ***Items*** |
| 1 | Standard is a minimum requirement issued by the Commissioner, for normal and recurring usage. It can also be defined as methods, guidelines or characteristics for activities or results of certain activities. The goal is to achieve the optimal level of the order in a given context. |
| 2 | This Personal Data Protection Standard is applicable to data users who are **not registered** with the Commissioner. |
| 3 | This Personal Data Protection Standard is applicable to the class of data users who **are registered** with the Commissioner. |
| 4 | This Personal Data Protection Standard shall be read together with Code of Practices for Class of Data Users registered by the Commissioner. |
| 5 | This Personal Data Protection Standard is effective immediately from the date of the Personal Data Protection Act 2010 was enforced. |
| **6** | **Overall feedback:** |

1. **SECURITY STANDARDS**

|  |  |  |
| --- | --- | --- |
| ***MANAGEMENT OF PERSONAL DATA MANAGED ELECTRONICALLY*** | | |
| ***No.*** | ***Items*** | ***Comments*** |
| 1 | Personnel who manages personal data should be registered in an efficient registration system prior to the authorization to access the personal data system. |  |
| 2 | The password for a user account should be changed within three (3) working days when the personnel no longer manages personal data. |  |
| 3 | Before a certain personnel is authorised to access the personal data system, the organisation must set the limit on authorisation for each personal data processing activity. This is to ensure that data are processed for certain activity only. |  |
| 4 | Revocation of authorised access must be executed when a personnel is no longer working in the organization within three (3) working days. |  |
| 5 | The record on use of data system should be maintained thoroughly each week. This should be implemented to monitor access to personal data. |  |
| 6 | Transfer of personal data by electronic means shall comply with the Principles of Personal Data Protection. Standard Operating Procedures (SOPs) must be developed in a clear and orderly manner. |  |
| 7 | The place for storing personal data shall be in an appropriate location which is secured and safe from physical threats and natural threats. |  |
| 8 | Data users must set physical security procedure such as follows:   1. Control the access to the data storage   area;   1. Set up closed circuit camera at the   data storage area (if necessary), and   1. Provide security service 24 hours a day (if necessary). |  |
| 9 | Data users should have Back up/Recovery System and the latest anti-virus software to protect customers’ data in the event of intrusion etc. |  |
| 10 | Data user is required to have control over malware and have the operating systems regularly scanned to avoid attacks on data stored electronically. |  |
| 11. | Transfer of personal data that are processed electronically should be blocked except with the permission of the authorised officers for related activity only. |  |
| 12 | A contract should be entered with the third party who process personal data on behalf of the data user. This is for the purpose of ensuring the security of personal data from loss, misuse, modification, unauthorised access and disclosure. |  |
| **13** | **Overall feedback:** | |

|  |  |  |
| --- | --- | --- |
| **PERSONAL DATA MANAGEMENT MANAGED CONVENTIONALLY** | | |
| ***No.*** | ***Items*** | ***Comments*** |
| 1 | Personnel who manages personal data needs to be registered in an efficient registration system before accessing customer's personal data. |  |
| 2 | Records of authorization to access personal data are to be maintained and managed by data user. |  |
| 3 | Authorisation to access data must be revoked within three (3) working days if the personnel is no longer involved in processing customer’s personal data, either move to other organisation or no longer working in the data user organisation. |  |
| 4 | Data users should set physical security procedure such as follows:   1. all personal data should be stored in files in an orderly manner; 2. all those files should be stored in locked cabinets and in a locked room; 3. all keys shall be kept in a safe   place;   1. only authorised personnel is allowed to keep the keys. While duplicate keys shall be kept in a place deemed safe and reasonable, and 2. The place for storing personal data   shall be in an appropriate location  which is secured and safe from  physical and natural threats. |  |
| 5 | Data users will need to update permissions to access data on a regular basis. This is to control and avoid accessing personal data by unauthorised personnel. |  |
| 6 | Data users must provide Letter of Undertaking of Confidentiality for personnel who are involved with the managing and processing personal data. |  |
| 7 | Data users can conduct awareness programme on the responsibility of protecting personal data to all personnel (if necessary) |  |
| 8 | Transfer of personal data by unconventional means shall comply with the Principles of Personal Data Protection. Standard Operating Procedures (SOPs) must be developed in a clear and orderly manner. |  |
| 9 | All used paper, printed documents or other documents which clearly show customers’ personal data need to be disposed of carefully and efficiently by using shredding machine or other suitable methods. |  |
| **10** | **Overall feedback:** | |

1. **STORAGE STANDARDS**

|  |  |  |
| --- | --- | --- |
| Data users should take reasonable steps to ensure that the customer's personal data is destroyed or deleted permanently if the personal data is no longer required to be kept. Storage of personal data should be well managed as follows: | | |
| **No.** | **Items** | **Comments** |
| 1 | Determine all legislations related to the processing and storage of personal data before destroy any personal data. |  |
| 2 | Personal data should not be kept longer than is necessary for any purposes. Thus, personal data should be disposed within a period not exceeding seven (7) days after commercial transaction has completed. |  |
| 3 | Different sets of data must be kept for a purpose/purposes that are specific, lawful and clearly stated and should be fairly processed in a manner compatible with each purpose. |  |
| 4 | Effectively supervise and report on the process of the disposal of personal data. |  |
| 5 | Data collection forms at the time of acquisition of personal data for the purpose of commercial transactions should be disposed off within a period not exceeding seven (7) days. |  |
| 6 | All personal data that are no longer needed must be deleted from the database. |  |
| 7. | Standard Operating Procedures (SOPs) about retrieval of personal data from the storage system must be developed in a clear and orderly manner. |  |
| 8 | Standard Operating Procedures (SOPs) about comprehensive security controls including maintenance of system and storage must be developed in a clear and orderly manner. |  |
| 9 | Having a proper and regularly maintained schedule for disposal of inactive personal data. |  |
| **OTHER MATTERS** | | |
| 10 | For security purpose, the use of personal pen drive or external hard disk are not allowed arbitrarily without written consent. |  |
| 11 | The use of personal pen drive or external hard disk for the purpose of data management as well as administration of the related system must be consented by top management. |  |
| **12** | **Overall feedback:** | |

1. **INTEGRITY DATA STANDARDS**

|  |  |  |
| --- | --- | --- |
| **MANAGEMENT OF PERSONAL DATA MANAGED ELECTRONICALLY** | | |
| Data user shall take reasonable steps to ensure that personal data are accurate, complete, not misleading and up-to-date with regard to the purpose, including any purpose related to direct, to whom the personal data collected and processed further. Such measures are: | | |
| **No.** | **Items** | **Comments** |
| 1 | Providing forms for updating of personal data to customers. |  |
| 2 | Updating customer’s personal data within seven (7) days after receiving notice of correction from customer. |  |
| 3 | Assessing or cross-check the appropriate supporting documents to determine the validity and accuracy of personal data. |  |
| 4 | Informing customers about personal data updating activities. Notice of update should be displayed in portal/website. |  |
| 5 | Displaying the notice on updating activities of personal data at the business premises. |  |
| 6 | Informing customers about the updates at times that fit within the appropriate and compatible methods. |  |
| **MANAGEMENT OF PERSONAL DATA MANAGED CONVENTIONALLY** | | |
| Data user shall take reasonable steps to ensure that personal data are accurate, complete, not misleading and up-to-date with regard to the purpose, including any purpose related to direct, to whom the personal data collected and processed further. Such measures are: | | |
| 1 | Providing forms for updating of personal data to customers. |  |
| 2 | Updating customer’s personal data within seven (7) days after receiving notice of correction from customer. |  |
| 3 | Assessing or cross-check the appropriate supporting documents to determine the validity and accuracy of the personal data. |  |
| 4 | Displaying notice on updating activities of personal data at the business premises. |  |
| 5 | Informing customers about the updates at times that fit within the appropriate and compatible methods. |  |
| **6** | **Overall feedback:** |  |

**\*\*The End\*\***