

Data Protection and Privacy Standards and Guidelines

Version: 1.0.0

Status: In Review

Date: 14 April 2024

Prepared by:			
Name	Metric number	Department	Date
Shengzhe Huang	S2193216	QA (Standard & Compliance)	14 April 2024
Muhammad Qaim Bin M. Baaden	S2100510	QA (Standard & Compliance)	14 April 2024
Approved by:			
Name	Metric number	Department	Date
Released by:			
Name	Metric number	Department	Date

Table of Contents

Table of Contents.....	2
1.0 Description.....	3
1.1 Purpose.....	3
1.2 Scope.....	3
2.0 Related Documents.....	3
2.1 References.....	3
3.0 Personal Data Protection Act (PDPA) in Malaysia.....	4
4.0 Scope of PDPA.....	4
5.0 Sensitive Data Under PDPA.....	4
6.0 Rights of Data Subjects.....	4
7.0 Data Protection Principles.....	5
8.0 Enforcement and Penalties.....	5
9.0 Conclusion.....	5

1.0 Description

1.1 Purpose

This documentation is tailored to establish comprehensive data privacy and protection guidelines for the development of the Optical Character Recognition (OCR) System for Handwritten Multiple-Choice Question (MCQ) Answer Sheet Evaluation project. It aims to provide standards, procedures, and design principles crucial for safeguarding sensitive data throughout the project's lifecycle.

This documentation also emphasized the importance of robust data privacy measures, this document serves as a reference for ensuring that user information is adequately protected and regulatory requirements are met

1.2 Scope

All data handling procedures implemented within the OCR database project's permanent repository shall strictly adhere to the data privacy and protection guidelines outlined in this document and its associated references. These guidelines are designed to ensure that all aspects of data management within the project comply with stringent privacy measures and regulatory requirements.

2.0 Related Documents

2.1 References

3.0 Personal Data Protection Act (PDPA) in Malaysia

According to the Personal Data Protection Act, users need to be protected to prevent any form of abuse against the storage or processing of personal data of individuals, public and private sectors in Malaysia for commercial transactions is stipulated under the PDPA.

4.0 Scope of PDPA

The PDPA applies to any person who processes or has control over the processing of personal data (referred to as 'data user'). It is pertinent to note that processing is defined widely under the PDPA to cover a wide range of activities, including using, disseminating, collecting, recording, and/or storing personal data.

5.0 Sensitive Data Under PDPA

Sensitive data: Sensitive personal data under the PDPA includes any personal data consisting of information as to the physical or mental health or condition of a data subject, their political opinions, their religious beliefs or other beliefs of a similar nature, the commission or alleged commission by them of any offense or any other personal data as the Minister may determine by order published in the Gazette. The obligations imposed by the PDPA in respect of sensitive personal data are more stringent.

[Malaysia - Data Protection Overview | Guidance Note | DataGuidance](#)

6.0 Rights of Data Subjects

Data subjects have several rights under the PDPA to maintain control over their personal data:

1. Right to Access: People may ask to see their personal information kept on file by data users to confirm its accuracy and comprehend how it will be used.
2. Right to Correction: Individuals who provide their personal data have the right to have any errors corrected.
3. Right to Withdraw Consent: If a data subject withdraws their consent, data users must stop processing their data unless there are compelling grounds to do otherwise.
4. Right to Data Portability: Individuals can transfer their personal data between service providers in an organized format.
5. Right to Object: Individuals who are the subjects of data may object to the processing of their personal information for purposes, such marketing.

[Personal Data Protection Act 2010 – Jabatan Perlindungan Data Peribadi \(pdp.gov.my\)](#)

7.0 Data Protection Principles

The PDPA outlines key principles that data users must adhere to when processing personal data:

- **Accountability Obligation:** Businesses need to make sure they have the right procedures in place to fulfill their PDPA-related duties. This entails appointing a Data Protection Officer (DPO) and providing information upon request on data protection policies, practices, and complaint procedures.
- **Obligation of Consent:** Personal information should only be gathered, utilized, or shared for reasons for which the individual has granted consent. Organizations are required to give people the option to revoke their consent and to advise them of the possible repercussions.
- **Purpose Limitation Obligation:** Only use, collection, and disclosure of personal data for purposes that a reasonable person would deem suitable in the circumstances at hand and with the individual's consent is permitted.
- **Consent Limitations: Obligation:** Only uses, collection, and disclosure of personal data for purposes that a reasonable person would deem suitable in the circumstances at hand and with the individual's consent may occur.
- **Accuracy Obligation:** Organizations have an obligation to ensure the accuracy and completeness of the personal data they collect.
- **Protection Obligation:** To guard against risks of unauthorized access, collection, use, disclosure, or other similar situations, reasonable security measures must be put in place.
- **Limit of Retention Obligation:** When personal information is no longer required, it must be properly disposed of and not kept for longer than is necessary for legal or business purposes.

[PDPC | Data Protection Obligations](#) (Note that while this source is from Singapore, the principles are applicable as well as what is outlined in the PDPA in Malaysia!)

8.0 Enforcement and Penalties

The Personal Data Protection Commissioner is authorized by the PDPA to ensure that its rules are followed. If proven to be in breach of the PDPA, data users risk fines and perhaps jail time. Moreover, anybody impacted by PDPA violations may file civil lawsuits to recover damages.

9.0 Conclusion

Malaysia's data protection environment has been greatly influenced by the PDPA, which guarantees the responsible, open, and safe handling of personal data. In addition to preserving people's right to privacy, PDPA compliance boosts consumer confidence in Malaysian companies.