MINISTRY OF DIGITAL

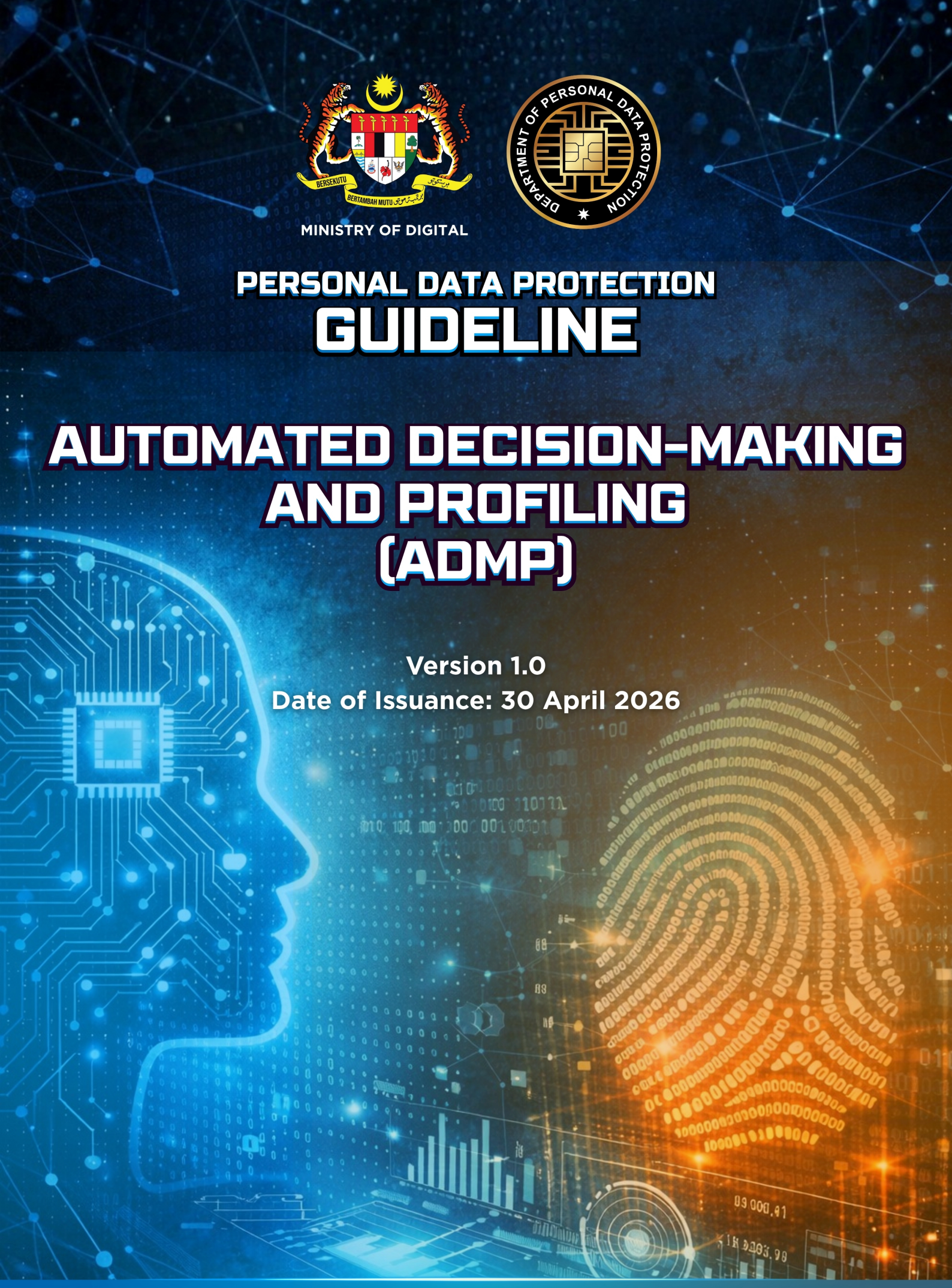
PERSONAL DATA PROTECTION

GUIDELINE

AUTOMATED DECISION-MAKING AND PROFILING (ADMP)

Version 1.0

Date of Issuance: 30 April 2026



DEPARTMENT OF PERSONAL DATA PROTECTION

Address:

DEPARTMENT OF PERSONAL DATA PROTECTION
Level 8, Galeria PjH, Jalan P4W, Persiaran Perdana
Precinct 4, Federal Government Administration Centre
62100 Putrajaya, Malaysia

TABLE OF CONTENTS

PART A: INTRODUCTION

1. Background

1.1 The Personal Data Protection Act 2010 ("**Act 709**") does not currently provide specific provisions to regulate or address the concept of Automated Decision-Making and Profiling ("**ADMP**"). Nevertheless, any personal data processing activities in commercial transactions, including those involving ADMP, shall comply with the provisions under Act 709, particularly the Personal Data Protection Principles.

1.2 This ADMP Guideline ("**Guideline**") provides guidance on the introduction and implementation requirements of ADMP. It adopts a balanced approach to support the Data Controller and the Data Processor in safeguarding the personal data of data subject while implementing innovative technologies in their business activities.

1.3 Where an organisation embarks on the implementation of ADMP, the Data Protection Officer(s) ("**DPO**") shall be engaged at the earliest possible stage. Such engagement shall commence with the carrying out of a Data Protection Impact Assessment ("**DPIA**") to ensure compliance with personal data protection requirements.

1.4 This Guideline supplements and is to be read together with Act 709 and any other relevant legislative instruments issued thereunder, as may be amended from time to time. This Guideline shall not be construed as overriding any other applicable laws or regulations relating to personal data protection in force.

1.5 Please note that the examples provided in this Guideline are for illustrative purposes only and are not intended to be exhaustive.

2. Legal Provisions

2.1 This Guideline is issued by the Personal Data Protection Commissioner ("**Commissioner**") pursuant to the functions of the Commissioner under subsection 48(g) of Act 709.

3. Interpretation

3.1 Unless otherwise defined in this Guideline, the terms and expressions used herein shall have the same meanings assigned to them under Act 709 and any other relevant legislative instruments issued thereunder.

3.2 In this Guideline, unless the context otherwise requires:

"Automated decision-making" or **"ADM"**	means the process of making decisions without any human involvement by wholly or partly automated means.
"Profiling"	means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a data subject, in particular to analyse or predict aspects concerning that data subject's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

PART B: INTRODUCTION TO AUTOMATED DECISION-MAKING AND PROFILING

4. Introduction to Automated Decision-Making and Profiling

4.1 ADM means the process of making decisions without any human involvement using wholly or partly automated means. “Without human involvement” could also include situations where human influence is minimal. In such circumstances, a process is still considered ADM if a human merely inputs the data to be processed, and an automated system carries out the subsequent decision-making.

4.2 Profiling means any form of automated processing of personal data involving the use of personal data to evaluate certain personal aspects relating to a data subject, in particular to analyse or predict aspects concerning that data subject. Two (2) elements in profiling distinguish this process from simple data categorisation or trend

analysis:

(a) **predictive elements**: personal data is used to predict or generate new insights relating to a data subject's personal characteristics; and/or

(b) **inference elements**: generalisations about populations from the sample data subject.

Examples:

(i) A financial institution deploys a fully automated system to evaluate loan applications by generating a probability score representing the applicant's creditworthiness based on personal data, including income, employment history, repayment records, age, residential address, and behavioural data such as spending patterns and digital footprint. Applications falling below a pre-set threshold are automatically rejected without human review.

ADM: Determine eligibility for financial service products.
Profiling: Predicting and inferring applicants' economic condition and financial reliability.

(ii) An e-commerce company monitors a data subject's online behaviour (e.g., browsing activity, frequency of purchases for specific categories) and creates a profile of the predicted individual's interests and preferences. This profile is used to determine the type of products to be marketed to the data subject and/or to determine the data subject's eligibility for certain discount rates.

ADM: Determining the data subject's eligibility for specific discount rates.
Profiling: Predicting and inferring potential buyers' interests and preferences.

(iii) The human resources department of a company uses an automated algorithm to process personal data for the purpose of selecting candidates for physical interviews. Based on this automated assessment, the algorithm ranks and shortlists candidates for interview.

ADM: Determining candidates' eligibility for interview using an algorithm.

Profiling: Predicting and inferring an applicant's suitability and potential performance at work for a given role.

(iv) A healthcare institution applies a machine learning system to determine patients' health status or the likelihood of a treatment being successful for a particular patient based on certain group characteristics (e.g., age, medical history, and lifestyle).

ADM: Determining the patient's health status or the likelihood of a treatment being successful.
Profiling: Predicting and inferring the likelihood of treatment success based on personal characteristics (e.g. age, medical history, lifestyle).

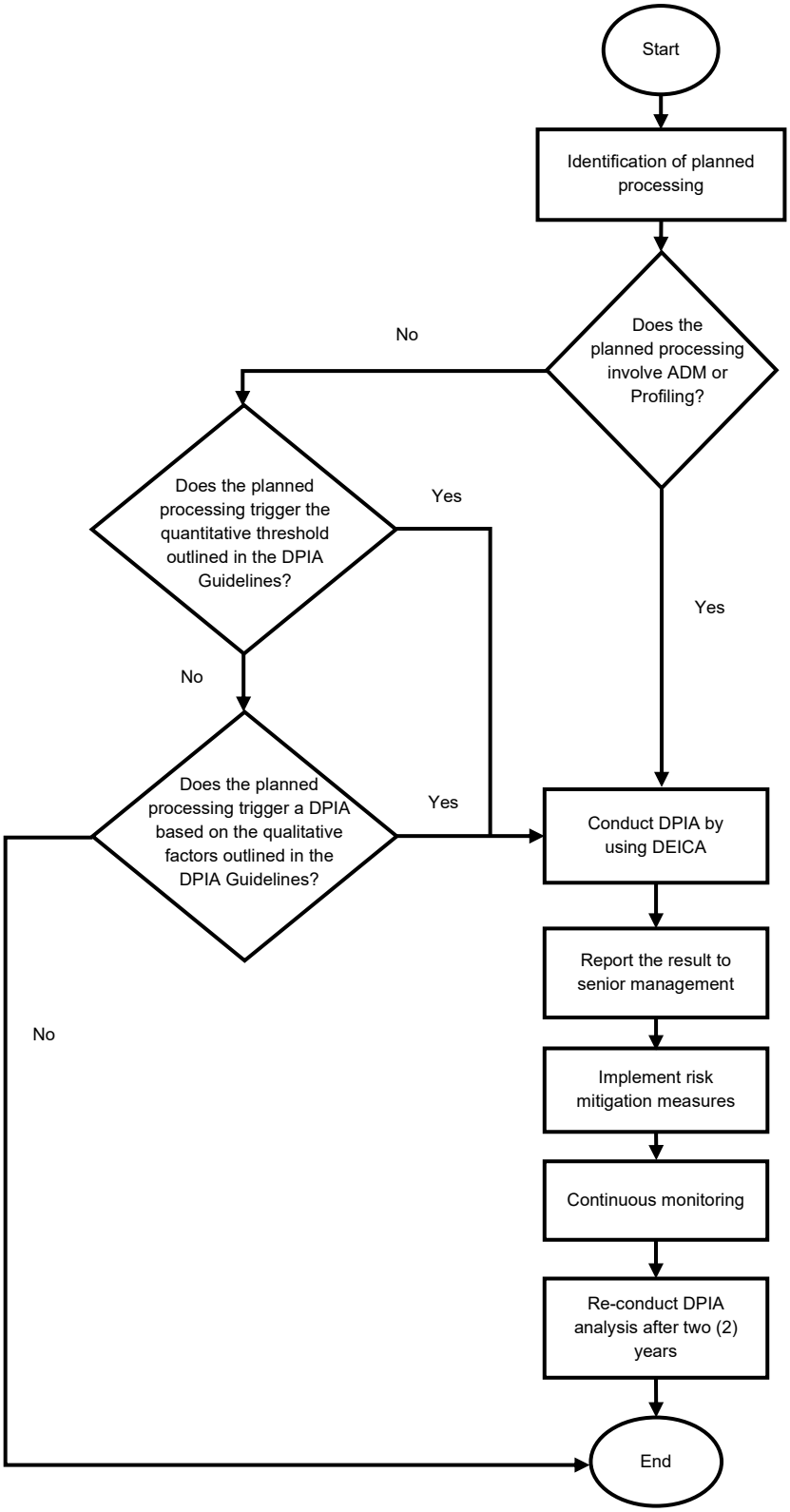
PART C: APPLICATION OF AUTOMATED DECISION-MAKING AND PROFILING

5. The Role of the Data Protection Officer (DPO) in ADMP

5.1 Where an organisation identifies the need to embark on the implementation of ADM and profiling, the DPO shall have specific responsibilities in overseeing ADMP systems. These responsibilities include supporting the carrying out of the DPIA (please refer to paragraph 6.0 to understand the relationship between ADMP and DPIA), and acting as the facilitator and point of contact between the data subject and the data controller or data processor regarding the processing of personal data and the exercise of applicable rights.

6. Relationship between ADMP and DPIA

6.1 ADMP is one of the qualitative factors that triggers the requirement to carry out a DPIA, regardless of the nature or extent of its intended use. Therefore, the DPO shall ensure a DPIA is carry out for any planned processing that includes ADMP elements. Please refer to the flowchart below.


Start
Identification of planned processing
Does the planned processing involve ADM or Profiling?
No
Yes
Does the planned processing trigger the quantitative threshold outlined in the DPIA Guidelines?
Yes
No
Does the planned processing trigger a DPIA based on the qualitative factors outlined in the DPIA Guidelines?
Yes
No
Conduct DPIA by using DEICA
Report the result to senior management
Implement risk mitigation measures
Continuous monitoring
Re-conduct DPIA analysis after two (2) years
End

7. Guideline Applicability

7.1 This guideline may not apply to all ADMP activities. Therefore, DPOs are required to exercise their best judgment when assessing whether the ADMP threshold is met in relation to any planned processing when applying this Guideline. The ADMP threshold is met where the outcome of the ADMP process may:

7.1.1 result in legal effects concerning the data subject; or
7.1.2 significantly affects the data subject,

(collectively, the "**ADMP Threshold**").

Legal effects concerning the data subject

7.2 The ADMP Threshold is met where the process produces a decision that may affect the data subject's legal status or legal rights. Such legal effects may include the termination of a contract or entitlement, or the rejection of a social benefit conferred by law.

Significantly affect the data subject

7.3 The ADMP Threshold is met where the process produces a decision that has a significant effect on the data subject, which may have the potential to:

7.3.1 significantly affect the circumstances, behaviour, or choices of the subject data concerned;
7.3.2 have a prolonged or permanent impact on the data subject; or
7.3.3 at its most extreme, leads to the exclusion or discrimination of the data subject.

7.4 Examples of such decisions include:

7.4.1 decisions that affect the data subject's financial circumstances, such as eligibility for credit;

7.4.2 decisions that affect the data subject's access to essential services such as health services;

7.4.3 decisions that deny the data subject an employment opportunity or place the data subject at a serious disadvantage;

7.4.4 decisions that result in one data subject being offered a more favourable (lower) price for a product compared to another data subject;

7.4.5 decisions that affect the data subject's access to education, such as university admissions; or

7.4.6 decisions that result in reputational harm.

Illustrations

(i) A financial institution deploys a fully automated system to evaluate loan applications by generating a probability score representing the applicant's creditworthiness, based on personal data including income, employment history, repayment records, age, residential address, and behavioural data such as spending patterns and digital footprint. Applications falling below a pre-set threshold are automatically rejected without human review.

ADM: Determine eligibility for financial service products

Profiling: Predicting and inferring applicants' economic condition and financial reliability.

Significantly affects circumstances	Automatic refusal of credit based solely on the probability score.
Prolonged or permanent impact	A single automated assessment may have lasting effects on the data subject.

(ii) A general insurance firm uses a fully automated profiling system in determining health insurance premiums based on the data subject's personal data, such as age, postal codes, and lifestyle. This approach has the potential to lead to group discrimination among applicants.

ADM: Determine the health insurance premium pricing.

Profiling: Predicting and inferring applicants' health conditions and insurance risk.

Significantly affects choices	Certain groups of the data subject may be offered less favourable (higher) premiums compared to other groups.
Prolonged/permanent impact	Insurance tiering decisions may be recurring and may influence access to healthcare over time.

(iii) The human resources department of a company uses an automated algorithm to process personal data in selecting candidates for physical interviews. Based on this automated assessment, the algorithm ranks and shortlists candidates for such interviews.

ADM: Determine interview eligibility using an algorithm

Profiling: Predicting and inferring candidate's suitability and potential performance at work for a given role.

Significantly affects circumstances	Automatic rejection may adversely affect employment opportunities and may contribute to long-term unemployment.
Prolonged or permanent impact	Such automated assessments may have lasting effects on the data subject's career prospects.

(iv) A talent platform uses a system that generates reputational rating indicators to measure the reliability of individuals in professional fields, based on personal data such as residential address and behavioural data, including digital footprint. These ratings are then shared with the platform's business customers as part of the data subject's credentials.

ADM: Determine the data subject's credentials.

Profiling: Predicting and inferring the data subject's expertise.

Significantly affects circumstances	A data subject flagged as “unreliable” may suffer reputational harm, which may adversely affect business and professional relationships.
Prolonged or permanent impact	Such reputational assessments may persist over time and have lasting effects on the data subject’s professional opportunities.

PART D: GENERAL GUIDANCE TO AUTOMATED DECISION-MAKING AND PROFILING

8. ADM and Profiling Involving Sensitive Personal Data

8.1 Section 40 of Act 709 provides that a data controller shall not process any sensitive personal data (including biometric data) of a data subject except in accordance with certain conditions. Such conditions include where the data subject has given explicit consent to processing, or where the processing is necessary in certain circumstances specified under subsection 40(1)(b) of Act 709, including, among others:

(a) employment law compliance;
(b) protecting the vital interests of the subject;
(c) medical purposes by a healthcare professional; or
(d) legal proceedings or obtaining legal advice.

8.2 In addition to obtaining prior explicit consent, a data controller may consider implementing strong safeguards when processing sensitive personal data. Such safeguards may include technical measures such as encryption of sensitive personal data, and organisational safeguards such as stricter access controls within the organisation.

8.3 These concepts will similarly apply to the processing of personal data for ADMP.

9. Compliance with Personal Data Protection Principles and Data Subject's Rights under Act 709

9.1 While Act 709 does not specifically address ADM or profiling, the Personal Data Protection Principles and the rights of data subject under Act 709 shall also apply to ADM and profiling, in particular:

9.1.1 Notice and Choice Principle; and

9.1.2 Withdrawal of Consent.

Notice and Choice Principle

9.2 In accordance with the Notice and Choice Principle under Section 7 of Act 709, the data controller shall, by way of a written notice, inform the data subject of the information relating to the processing of the data subject's personal data.

9.3 If such processing also involves ADM or Profiling, the data controller shall inform the data subject of this information.

9.4 The Data Controller may, in the written notice provided to the data subject, describe the types of decisions made through ADM or profiling, the reasons for such decisions, and the possible consequences of those decisions. The level of information provided should be as extensive as is reasonably practicable, but need not include any confidential information, trade secrets, intellectual property, proprietary rights, or other similar information.

9.5 These written notices shall be easily accessible to the data subject and updated as soon as practicable in line with the evolution of ADMP activities.

Withdrawal of Consent to process personal data

9.6 In accordance with Section 38 of Act 709, it shall be the data subject's right to withdraw consent to the processing of personal data by notice in writing and the data controller, upon receiving such written notice, shall cease the processing of the personal data.

9.7 The data subject shall retain the right to withdraw consent to the processing of personal

data, including where such processing involves ADMP. The data subject may withdraw such consent by giving a written notice to the data controller, and upon receipt of such notice, the data controller shall cease the processing of the data subject's personal data that includes ADM or Profiling.

9.8 The data controller implementing ADMP systems shall ensure that accessible, straightforward, user-friendly mechanisms and processes are established to enable the data subject to exercise this right. The data subject's right to withdraw consent, including the mechanisms and processes available for exercising such right, shall also be made known to the data subject.

Exceptions

9.9 ADMP may be undertaken in the following circumstances:

9.9.1 where the processing is necessary for entering into, or performance of, a contract between the data subject and the data controller;

9.9.2 where the processing is necessary for compliance with laws; or

9.9.3 where the data subject has given prior consent.

(collectively, the "**Exceptions**").

9.10 To enable the data controller to rely on any of the Exceptions described above, consent must be obtained from the data subject for the purposes of the processing of personal data, which also applies if the processing includes ADMP.

9.11 Compliance with laws referenced in Paragraph 8.1 includes a reference to subsection 40(1)(b) of Act 709. This means that ADMP involving sensitive personal data may be undertaken if any of the applicable legal bases under subsection 40(1)(b) of Act 709 applies.

Exemptions

9.12 Part III of Act 709 sets out exemptions from certain provisions of Act 709, which similarly apply to the processing of personal data involving ADMP (collectively, "**the Exemptions**").

PART E: ADOPTION OF ARTIFICIAL INTELLIGENCE IN AUTOMATED DECISION-MAKING AND PROFILING

10. Artificial Intelligence

10.1 It shall be noted that not all processing of personal data involving ADM or profiling utilises Artificial Intelligence, including Generative Artificial Intelligence ("**AI**"). This Guideline is to apply only where AI is used for the processing of personal data involving ADMP.

10.2 The data controller may adopt the following best practices for the use of AI in ADMP:

10.2.1 identify the commercial objectives of using AI and assess the associated risks to the organisation's decision-making processes before deploying the AI;

10.2.2 use AI for Profiling in a manner that respects the data subject's dignity, ensure accurate outputs, acknowledge the limitations of AI, consider all potential adverse impacts, and restrict the use of AI to only its intended purpose(s);

10.2.3 inform the data subject of the use of AI in the processing of personal data involving ADMP when providing a written notice (personal data protection notice or privacy notice) regarding such processing. The data controller may consider the appropriate scope of the explanation on the use of AI in such notice, ensuring that it is not excessively lengthy or overly technical for the data subject;

10.2.4 consider and implement appropriate measures to mitigate the risks of over-dependence on AI systems or services when developing, providing, or using AI for ADMP;

10.2.5 provide appropriate training to the relevant personnel, particularly in risk assessment, compliance oversight, regulatory requirements, and data subject management, to ensure proper understanding and adequate knowledge of the operations and limitations of AI;

10.2.6 AI must not be relied upon as the sole factor when making policies and/or decisions concerning a data subject; and

10.2.7 relevant personnel may be designated as reviewers of AI used in ADMP. With appropriate training, such reviewers should be proactive, purposeful, authoritative, and competent in the evaluation and interpretation of AI use.