PUBLIC CONSULTATION PAPER NO. 3/2025:

AUTOMATED DECISION MAKING AND PROFILING GUIDELINE

Start Date: 20 March 2025

End Date: 19 May 2025

PART 1: INTRODUCTION AND BACKGROUND

[A] Introduction

1.1 Section 5 of Personal Data Protection Act 2010 ("**Act 709**") provides that the processing of personal data by a data controller shall comply with the prescribed personal data protection principles. However, the Act 709 does not specifically address automated decision making and profiling.

1.2 As technology advances, more processing and decisions are being made automatically. By using technology such as Artificial Intelligence ("**AI**") and machine learning techniques, other information (including highly sensitive information) can be predicted from non-sensitive data. For example, just by looking at information about someone's online behaviour, algorithms can guess or figure out things like their health, political views, or family life. This process is called profiling. These predictions can then be used for automated decision making, which can have a significant impact on individuals' lives.

1.3 Several jurisdictions including the European Union ("**EU**"), United Kingdom ("**UK**"), South Korea, Philippines, Indonesia and China have implemented requirements in relation to automated decision making and profiling in their data protection legislation and framework.

1.4 To ensure that Malaysia's personal data protection regulatory framework remains current, effective and aligned with the global data protection regulatory landscape, the Personal Data Protection Commissioner ("**Commissioner**") is developing the Automated Decision Making and Profiling Guideline ("**ADMP Guideline**"). The ADMP Guideline will provide guidance on the introduction and implementation requirements for automated decision making and profiling.

1.5 This Public Consultation Paper ("**PCP**") PCP seeks to gather public views and feedback regarding aspects that will be or should be addressed in the proposed ADMP Guideline. This PCP will also assist the Commissioner in determining the readiness of data controllers or data processors if the provisions of automated decision making and profiling are introduced and enforced under the Act 709.

PART 2: PROPOSED INTRODUCTION AND REQUIREMENTS FOR AUTOMATED DECISION MAKING AND PROFILING

2.1 As an overview, Part 2 of this PCP is categorised as follows:

(a) Introduction of Automated Decision Making and Profiling;

(b) Trigger for Regulation;

(c) How to Regulate:

(i) The Right to Refuse
(ii) The Right to Information
(iii) The Right to Human Review

(collectively, "**ADM Restrictions**");

(d) Exceptions to ADM Restrictions;

(e) Use of Personal Data for AI Training and Output;

(f) Biometric Data; and

(g) CCTV.

[A] Introduction to Automated Decision Making and Profiling

2.2 **Background:** The concept of automated decision making and profiling is currently not addressed under the Act 709.

2.3 "**Automated Decision Making**" is generally explained as the process or ability to make decisions by automated means without any human involvement.

2.4 "**Profiling**" is described by the Oxford dictionary as: "the recording and analysis of a person's psychological and behavioural characteristics, so as to assess or predict their capabilities in a certain sphere or to assist in identifying categories of people". In general, profiling involves collecting data about a person or group and examining their traits or behaviour patterns to categorize them or predict their abilities, interests, or likely behaviours. Essentially, it's a way to create a detailed picture of someone based on various data.

Examples of use cases:

(a) Financial institution (such as a bank) conducts automated processing of applications (containing personal data of the applicants) for financial service products (e.g. credit card) to determine eligibility of such individuals to these products without human assessment.

(b) An e-commerce company monitors an individual's online behaviour (e.g. browsing activity, frequency of purchases for specific categories) and creates a profile of the individual's interests to determine the type of products to be marketed to the individual and/ or determine the eligibility of such an individual to (less or more) discounts.

(c) The HR departments of companies seek to filter out candidates for a physical interview using an algorithm (where the algorithm's criteria may not be clear to the HR person) resulting in only 10 candidates of a certain race and background being selected.

(d) Applying machine learning to predict patients' health or the likelihood of a treatment being successful for a particular patient based on certain group characteristics (e.g. age, medical history, lifestyle).

(e) Digital twins are virtual models of real-world things like assets, people, or processes. They help organisations make better decisions by simulating strategies and behaviours. By constructing scenarios of real-world situations and outcomes, they can provide insights that serve as an early-warning system, predicting events and the likelihood they will occur. They also provide a risk-free digital laboratory for testing designs and options, improving efficiency and time to market, for example, by optimizing scheduling, sequencing and maintenance.[1]

2.5 Introducing the requirements on automated decision making and profiling in Malaysia will:

(a) improve and offer better data protection to data subjects, especially considering the risks due to rapid economic development and technological advancements; and

(b) bring our personal data protection standards in line with global standards and legislations.

[1] https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/digital-twins-and-generative-ai-a-powerful-pairing

2.6 **Proposal:** It is proposed that the concepts of automated decision making and profiling is introduced in the data protection framework in Malaysia. In this regard, the following definitions are proposed:

"**Automated decision making**" to be defined as: "Process of making decisions by automated means without any human involvement".

This definition is generally based on the definition adopted by the data protection authorities in certain countries – for context:

(i) **EU:** "Automated decision-making has a different scope and may partially overlap with or result from profiling. Solely automated decision-making is the ability to make decisions by technological means without human involvement."

(ii) **UK:** "Automated decision-making is the process of making a decision by automated means without any human involvement."

(iii) **Philippines**: "**Wholly or partially** automated processing operation that can make decisions using technological means totally independent of human intervention; automated decision-making often involves profiling"

(iv) **China**: "Refers to the activities of automatically analysing and evaluating personal behaviours, hobbies, or economic, health, and credit status, among others, through computer programs, and making decisions."

Explanation:

"automated means" refers to automated data processing using technology, where human influence is either excluded or very minimal. To illustrate, the use of AI and machine learning tools for data processing will be regarded as "automated means".

May involve profiling but does not have to (i.e. automated decisions can be made with or without profiling). For instance, automated systems can detect and block fraudulent transactions by analyzing patterns and anomalies in transaction data using predefined rules and algorithms, without profiling the user. However, if the systems starts to monitor and analyze the user's transaction history over time and build a profile of their typical behaviour, this would be considered profiling. For example, the system tracks the user's spending habits, preferred merchants, and typical transaction times, assesses the risk based on whether the user has a history of disputed transactions or previous fraud incidents, and applies different rules or thresholds for flagging transactions based on the user's profile. In this scenario, the decision to flag a transaction would be influenced by the user's profile, including their past behaviour and risk level, making it a profiling-based decision.

Profiling: "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."

This definition is generally based on the definition adopted by the data protection legislation or authorities in certain countries – for context:

(i) **The EU, UK** and **Philippines** adopt the same definition as the above.

(ii) **Indonesia** adopts a slightly different definition i.e.: "Any activity to identify an individual, including but not limited to work history, economic condition, medical records, personal preference, interest, talent, behaviour, location or movement of the data subject."

Question 1

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) What are your views on introducing the concepts of automated decision making and profiling in the data protection framework in Malaysia?

(b) What are your views on the proposed definitions for "automated decision making" and "profiling" as referred to in Paragraph 2.6? Do you think the definitions are too broad or too narrow?

(c) In particular, for the definition of "automated decision making", should processing be wholly or partly automated or simply just "automated" in order to be considered as "automated decision making"?

(d) When, how and why does your organisation carry out automated decision making and profiling?

(e) Do you agree that there has to be a predictive element (i.e. that the personal data is used to analyse or predict aspects relating to a person), or some degree of inference (i.e. drawing conclusions about individuals based on the data collected) for the processing to be considered profiling?

[B] Trigger for Regulation

2.7 **Background:** Automated decision making (and by extension profiling) by itself may not be harmful if it has no real impact on the individual.

Examples:

(a) Researchers may collect personal data of a group of individuals living in the city versus in the suburbs and use automated system to profile individuals who have a preference for living in the city versus the suburbs for sociological studies. This is used to understand broader social trends rather than affecting any specific person.

(b) A company may input the personal data of its subscribers into an automated system to enable it to derive data on "customer stickiness" (i.e. how likely customers are to continue using their services) (and what contributes to such a data point) to better improve its services overall (versus improve services for only selected categories of users which may be discriminatory). The process is to enhance the general user experience without discriminating against any particular category of users, thus having no adverse impact on specific individuals.

2.8 In the countries which have specific provisions on automated decision making and profiling in their respective personal data protection laws (e.g. EU, UK, South Korea, Indonesia and China), a risk-based approach is taken e.g. the data subject has the right not to be subject to or object a decision based solely on automated decision making, including profiling which **produces legal effects concerning the data subjects or similarly significantly affects the data subject.** Such approach balances the benefits of automated decision making with the need to protect individual from potential harm.

2.9 **Proposal:** It is proposed that automated decision making (and by extension profiling) should only be regulated if its use results in **legal effects concerning the data subject or significantly affects the data subject.**

Explanation:

*"**use results in legal effects concerning the data subject**": something that affects a person's legal status or their legal rights (e.g. cancellation of contract or entitlement or denial of social benefit granted by law).*

*"**significantly affects the data subject**": produces an effect that is equivalent or similarly significant in its impact (e.g.: automatic refusal of an online credit application or e-recruiting practices without human intervention). The decision must have the potential to:*

(a) *significantly affect the circumstances, behaviour or choices of the individuals concerned;*

(b) *have a prolonged or permanent impact on the data subject; or*

(c) *at its most extreme, lead to the exclusion or discrimination of individuals.*

Examples of such decisions include:

(a) *decisions that affect someone's financial circumstances, such as their eligibility to credit;*

(b) *decisions that affect someone's access to health services;*

(c) *decisions that deny someone an employment opportunity or put them at a serious disadvantage;*

(d) *decisions that result in one data subject being provided with a better price for a product compared to another individual;*

(e) *decisions that affect someone's access to education, for example university admissions.*

2.10 Therefore, what is proposed to be regulated are decisions which are:

(a) being made by technological means without human involvement; and

(b) where such decisions may legally or significantly affect an individual.

Question 2

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) Do you think there should be a trigger on regulation or do you think that any automated decision making and profiling (irrespective of whether it has any effect or impact) should be regulated?

(b) Do you agree with the proposed trigger for regulation i.e. automated decision making (and by extension profiling) should only be regulated if its use results in legal effects concerning the data subject or significantly affects the data subject? If not, what other triggers do you think should be applicable?

(c) In your view, what other thresholds or examples should be considered in determining what decision has a significant impact on data subjects?

(d) Should the same approach as EU Digital Services Act ("DSA") be adopted, in that the processing of sensitive personal data (including biometric data) should be completely restricted from profiling?

For context, under the DSA, advertisements based on "profiling" of GDPR "special category" data are banned under the DSA. Article 26(3) of the DSA provides: "Providers of online platforms shall not present advertisements to recipients of the service based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 using special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679"

"Special category" data is very broad, meaning personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or data concerning an individual's sex life or sexual orientation.

[C] How to Regulate

2.11 **Background:** There are a number of countries (including the EU, UK, South Korea, Philippines, Indonesia and China) which have specific provisions on automated decision making and profiling in their respective personal data protection laws.

2.12 Common rights or restrictions adopted by some of these countries include (some form of):

(a) the right to object or not to be subjected to a decision based solely on automated decision making (including profiling) which produces legal effects concerning the data subjects or significantly affects the data subject;

(b) the right to information / transparency requirement; and/or

(c) the right to request human review of the automated decision making.

2.13 **Proposal:** It is proposed that a data subject should be provided with:

(a) the right to refuse to be subjected to a decision based solely on automated decision making (including profiling) which produces legal effects concerning the data subjects or significantly affects the data subject ("**Right to Refuse**");

(b) a right to information on the automated decision making being undertaken (i.e. the transparency requirement) ("**Right to Information"**); and

(c) a right to request a human review of the automated decision making ("**Right to Human Review**"),

(collectively, the "**ADM Restrictions**").

Explanation:

(a) Rights to Refuse: *Data subjects have the right to refuse such processing which is:*

(i) ***"based solely on automated decision making****": a decision-making process that is entirely automated such that a human influence is excluded.*

A process might still be considered solely automated if a human merely inputs the data to be processed, and then the decision-making is carried out by an automated system.

"***use results in legal effects concerning the data subject***" (*see Example under Paragraph 2.9 above)*

(ii) "***significantly affects the data subject***" (*see Example under Paragraph 2.9 above)*

(b) Right to Information

(i) Where the processing involves automated decision making, this should be notified to the data subject.

(ii) In providing such information, data controllers must:

- *provide meaningful information about the logic involved; and*
- *explain the importance and potential impact of the processing.*

(iii) "Meaningful information about the logic" – should focus on describing:

- *the type of information collected or used in creating the profile or making the automated decision;*
- *why this information is relevant; and*
- *what the likely impact is going to be/how it's likely to affect the data subjects.*

(c) <u>Right to Human Review</u>

(i) Any review must be carried out by someone who has the appropriate authority and capability to change the decision. The reviewer should conduct a thorough assessment of all the relevant data, including any additional information provided by the data subject.

(ii) Data controller must provide an appropriate mechanism for the data subject to exercise these rights and/or a process in place for individuals to challenge or appeal a decision, and the grounds on which they can make an appeal.

(iii) If requested, data controller must provide justification and/or reason on the decision made.

(iv) Such requests should be acted upon within specific timelines (e.g. upon request within twenty-one (21) days of receipt or extend time by fourteen (14) days if the request is complex or multiple requests received from individual).

<u>Question 3</u>

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) As a data controller, have you encountered or do you foresee any potential challenges or difficulties in complying with the ADM Restrictions?

(b) Do you consider that aside from the proposed ADM Restrictions, is there any other rights or restrictions that should be introduced? E.g. should additional safeguards be put in place to prevent discriminatory effects?

For example, in China, prior to adopting automated decision-making measures, personal information processors should carry out a personal information protection impact assessment and keep the relevant records for at least three years. Meanwhile, in Philippines, a personal information controller must ensure that there are safeguards against the harms of extensive profiling such as discriminatory outcomes and infringement on the right to fair treatment and (where it carries out any automated decision-making operation or profiling) also register with the National Privacy Commission and identify the data processing system involved in the automated decision-making or profiling operation.

(c) In respect of the Right to Refuse, in your opinion, what are the operational difficulties in implementing such right?

(d) In respect of the Right to Information, in your opinion:

(i) What are the operational difficulties in implementing such right?

(ii) What level of detail or information do you think should be provided to comply with the Right to Information?

(e) In respect of the Right to Review, in your opinion:

(i) Do you think there should be any specific methods or process to be used by a data controller to justify why a decision is reached? If so, what are some examples?

(ii) Are the proposed timelines (referred to in the illustration at Paragraph (c)(iv) in the Explanation) to respond to the request to review adequate or should they be shortened / lengthened?

(f) Should targeted advertising (derived from profiling) towards children / minors be prohibited as per the EU's DSA?

For context, under the DSA, online platforms must not display advertisements to a user (whether on websites or mobile apps) based on profiling using that user's personal data, if they are aware "with reasonable certainty" that the user is a minor, although they are not required to process additional personal data to assess whether or not the user is a minor.

[D] Exceptions to the ADM Restrictions

2.14 **Background:** Other countries including the EU, UK, and South Korea, allow for some form of exceptions to the ADM Restriction in certain circumstances, e.g. (i) where the processing is necessary for entering into, or performance of, a contract between the data subject and a data controller, (ii) where necessary for compliance with laws, and (iii) the data subject has given prior explicit consent. Note that there are other countries which also provide different exceptions e.g.:

(a) in the Philippines no restrictions shall apply to automated data processing or profiling where there is another lawful basis for processing (other than consent or legitimate interest); and

(b) exceptions in Indonesia include national security and defence, law enforcement, public interest in the context of state administration etc.

Meanwhile, countries such as China does not appear to provide for any exceptions.

Further, in the EU and UK, where the automated decision making is based on the exceptions mentioned above, it must not be based on special categories of personal data unless:

(a) the data subject has given explicit consent to the processing of the personal data **or** processing necessary for reasons of public interest, on the basis of Union or Member State law or domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject; **and**

(b) suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

2.15 **Proposal:** It is proposed that automated decision making and profiling should be allowed in the following circumstances:

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

(b) necessary for compliance with laws; and

(c) data subject has given prior explicit consent;

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

Where the Exceptions apply, the Right to Refuse or Right to Human Review will not need to be provided to the data subject. However, it is proposed that the Right to Information still remains (i.e. the Exceptions will not apply to this).

2.16 While the above is generally based on the common approach taken by certain countries with respect to exceptions, it is proposed that the need for Right to Information is retained (i.e. not subject to the Exceptions) as there should be some form of transparency to the decision making process for the data subjects' benefit so that any explicit consent (falling within the Exceptions) is informed and can be granted.

2.17 It is also proposed that automated decision making that involves sensitive personal data is only allowed where:

(a) explicit consent from the data subject has been obtained or the processing is necessary for reasons of public interests; and

(b) the data controller has put in place suitable measures to safeguard the data subject's rights.

2.18 To enable a data controller to exclude the Right to Human Review and Right to Refuse, it is also proposed that "explicit consent" (rather than just consent) be provided to automated decision making in Malaysia. This means that the consent must be clear, specific and require a direct action from the data subject (e.g. checking a tick box or signing a document to indicate their consent).

2.19 Additionally, it is also proposed that all the ADM Restrictions will not apply for automated decision making and profiling in the following circumstances (some of which already apply for general processing under Section 45 of Act 709):

(a) personal data processed for individual's personal, family or household affairs, including recreational purposes;
(b) personal data processed for the:

(i) prevention or detection of crime or for the purpose of investigations;

(ii) apprehension or prosecution of offenders; or

(iii) the assessment or collection of any tax or duty or any other imposition of a similar nature;

(c) personal data processed for preparing statistics or carrying out research, provided that such personal data is not processed for any other purpose and that the resulting statistics or the results of the research are not made available in a form which identifies the data subject;

(d) personal data that is that is necessary for the purpose of or in connection with any order or judgement of a court;

(e) personal data processed for the purpose of discharging regulatory functions;

(f) processed only for journalistic, literary or artistic purposes, provided that:

(i) the processing is undertaken with a view to the publication by any person of the journalistic, literary or artistic material;

(ii) the data controller reasonably believes that, taking into account the special importance of public interest in freedom of expression, the publication would be in the public interest; and

(iii) the data user reasonably believes that in all the circumstances, compliance with the provision in respect of which the exemption is claimed is incompatible with the journalistic, literary or artistic purpose.

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

Such Exemptions are based on the existing Section 45 Exemptions under the Act 709 and are proposed on the basis that they are generally consistent with the general exemptions set out under the laws of the other countries. There are also instances where personal data protection principles should not apply e.g. either because there is a more important interest (e.g. for safety or legal purposes) or because the processing may not have significant impact (e.g. if processed for non-commercial purposes or the research does not end up identifying the specific individual).

Question 4

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) What are your views on the proposed Exceptions and Exemptions set out above? Do you think there should be any exceptions or exemptions in the first place?

(b) Do you consider the Exceptions to be adequate or should more exceptions be introduced? If yes, please provide any other exception to be considered.

(c) Do you think that the Right to Information should be retained and not subject to the Exceptions and Exemptions to ensure transparency in the decision-making process?

(d) Do you agree that automated decision making involving sensitive personal data which is based on any of the Exceptions should only be allowed where both of the following criteria are fulfilled:

(i) explicit consent from the data subject has been obtained or the processing is necessary for reasons of public interests; and

(ii) the data controller has put in place suitable measures to safeguard the data subject's rights?

[E] Use of Personal Data for AI Training and Output

2.20 **Background:** The regulation of AI varies across countries. Some places such as the European Union and China, have established comprehensive laws governing AI, while others have issued non-binding guidelines. These laws and guidelines do cover data protection to a certain extent, and certain data protection authorities have also issued specific guidelines on AI and data protection.

2.21 The machine learning/large language models that power AI and Generative AI rely on data (including personal data) for training and output purposes.

Examples:

The example below shows how machine learning models use data, including personal data, to train and generate output, improving their ability to provide accurate and relevant responses:

Virtual Assistant for Customer Support (e.g. chatbots)

(a) ***Training Phase:***

- *Data Collection: The virtual assistant is trained on a large amount of text data, including customer service interactions, FAQs, product manuals, and more. This data includes anonymized personal data, such as common customer queries and responses.*

- *Model Training: Machine learning algorithms analyze this data to learn patterns, such as how to respond to different types of questions, the appropriate tone to use, and the most relevant information to provide.*

(b) ***Output Phase:***

- *User Interaction: When a customer asks a question, the virtual assistant uses its trained model to understand the query and generate a response. For example, if a customer asks about the status of their order, the assistant can provide an update based on the information it has learned.*

- *Personalization: If the virtual assistant has access to the customer's history (with consent), it can provide more personalized responses. For instance, it might say, "Your order #12345 is on its way and should arrive by tomorrow," based on the customer's order history.*

(c) ***Profiling Aspect:***

- *Non-Profiling: The assistant responds based on general patterns learned during training, without considering the specific user's history. For instance, when a customer asks how to reset his/her password, the assistant replies with a general answer based on the patterns it learned during training: "To reset your password, go to the login page and click on 'Forgot Password.' Follow the instructions sent to your email to create a new password".*

- *Profiling: The assistant tailors its responses based on the user's past interactions and preferences, providing a more personalized experience. For example, it*

might use the customer's name, reference previous orders, or suggest products based on past purchases.

2.22 It should be noted that not all use of AI (including Generative AI) will involve automated decision making and profiling. For instance, an AI chatbot typically generates responses based on patterns learned from training data without making decisions about users or their actions. However, AI may be used for automatic decision making purposes i.e. AI systems (relying on large amount of personal data) can analyse complex datasets to identify patterns, predict outcomes, and make decisions based on this analysis.

2.23 There are some data protection concerns with AI and Generative AI which the ADM Restrictions can help address, including:

(a) AI development uses a lot of data which likely includes different kinds of personal information and sensitive information. Users may not know how their personal information is processed and it can therefore be difficult for them to exercise their rights. The Right to Information can reduce some of these issues; and

(b) building AI tools involve processing training data to build models that do recognise patterns. The original training data, the pre-trained model, and the output may all potentially contain personal information which may be difficult to access or correct, and may risk disclosure or influencing outcomes for a person in response to particular prompts. The ADM Restrictions can reduce some of these risks.

2.24 **Proposal:** It is proposed that use of AI and Generative AI (whether to train large language models or as part of obtaining an output from such models) should be expressly identified as an "automated decision making" tool. As such, the use of AI and Generative AI by data controllers which have legal effects on the data subject or significantly impacts the data subject should t be subject to the ADM Restrictions.

Examples:

The following are examples of how the use of AI and Generative AI can significantly impact data subjects:

*(a) **Financial Services**: Generative AI models can analyze large amounts of financial data to determine creditworthiness. Decisions made by these models can affect a person's ability to obtain loans, mortgages, or credit card.*

*(b) **Healthcare Diagnostics**: AI can predict the likelihood of diseases based on patient data, impacting insurance premiums and eligibility.*

(c) ***Law Enforcement and Surveillance****: AI systems used in surveillance can identify individuals in public spaces, impacting privacy and civil liberties.*

(d) ***Social Benefits and Welfare****: AI can be used to determine if an individual is eligible for social benefits such as unemployment insurance, disability benefits, and welfare programs. Generative AI can automate the processing of applications and claims. Errors or biases in these AI systems can result in wrongful denial of benefits, directly impacting individuals' financial stability and well-being.*

2.25 Specifically for the use of AI and Generative AI triggering ADM Restrictions, it is proposed that the following additional principles or measures should be considered and implemented by data controllers:

(a) when using AI for profiling, where it can significantly affect personal rights and benefits, the AI should be used in a way which respects the dignity of individuals, maintaining the utmost accuracy of the output, understanding limitations of the AI's predictions, recommendations, and judgments and to carefully consider possible disadvantages and not use it for inappropriate purposes.

(b) do not develop, provide, or use AI systems and services to manipulate human decision making, recognition and emotion or to control them without their awareness. When developing, providing, or using an AI system or service, pay attention and take necessary countermeasures against the risk of depending too much on AI, such as automated biases.

(c) before deploying AI solutions, data controllers should decide on their commercial objectives of using AI, and then weigh them against the risks of using AI in the organisation's decision-making.

(d) where the AI system is intended for autonomous decision making, provide training or a clear explanation to ensure that organisations using the AI system properly understand how the AI system operates.

(e) ensure that AI is not implemented as the only factor in making policies and/or decisions concerning people, to prevent the occurrence of racism and avoiding any action that harms people.

(f) human reviewers must check the system's recommendation and should not just apply to individuals automatically. Reviewers' involvement must be active and not just for show. They should have actual 'meaningful' influence on the decision, including the 'authority and competence' to go against the automated recommendation. Reviewers must 'evaluate' and 'interpret' the recommendation, consider all available input data, and also take into account other additional factors.

Question 5

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) What are your views use on AI and Generative AI automatically being considered as an "automated decision making" tool and therefore subject to the ADM Restrictions (where their use have legal effects on the data subject or significantly impacts the data subject)?

(b) What are your views on the additional principles or measures set out in Paragraph 2.25 above? For instance, do you consider such measures to be necessary and/or sufficient to address the risk of the use of AI and Generative AI or whether such principles are too onerous on data controllers, and may hold back innovation?

(c) As a data controller, to the extent that you use AI and Generative AI, do you foresee any potential challenges or difficulties in implementing such proposed additional principles or measures? If so, what are the ways to address or mitigate such challenges or difficulties?

(d) Are there currently any AI standards or guidelines (which contains requirements relating to personal data and ADM) that may be imposed on data controllers within a particular sector /industry? If your answer is yes, please specify the sector / industry you are referring to along with details of such standards or guidelines.

[F] Biometric Data

2.26 **Background:** Section 4 of Act 709 (as amended) introduces:

(a) the inclusion of “biometric data” into the definition of “sensitive personal data”; and

(b) a new definition for “biometric data” i.e. “any personal data resulting from technical processing relating to the physical, physiological or behavioural characteristics of a person”.

2.27 To supplement the above, the ADMP Guideline will provide additional guidance on interpretation of “biometric data” and include measures that data controllers should implement when processing biometric data.

2.28 Biometric data is generally treated as a special category of personal data or sensitive personal data (e.g. in places such as EU, UK, Australia, Indonesia, and China) and some

data protection authorities have issued specific guidelines, report, drafts, opinions and similar documents ("**Guidance**") relating to the use of biometric data.

2.29 Note that under the EU Digital Services Act, biometric data (as defined under the EU GDPR) cannot be used for profiling.

2.30 **Proposal:** It is proposed that the categories of personal data which fall within the definition of "biometric data" is clarified and additional safety measures should be taken by data controllers when processing biometric data (whether for use in automated decision making with legal effects or significant effects on the data subject or otherwise).

2.31 In particular, it is proposed that the following should be considered as examples of biometric data:

(a) Fingerprint;
(b) Facial recognition;
(c) Iris and Retina Scans;
(d) Voices / Voice Recognition;
(e) DNA;
(f) Handwriting; and
(g) Gait (i.e. a person's manner of walking).

2.32 Other than the current measures under the Act 709 and ADM Restrictions, the following additional measures are proposed for processing biometric data (even where ADM Restrictions are not triggered):

(a) Transparency and control – To inform the data subjects about, among others, how their biometric data is used and control over their biometric information.

(b) Security - impose appropriate security measures and technical safeguards such as encryption. To prevent identity spoofing (i.e. use of a synthetic object (e.g. synthetic fingerprint, 3D model of a face) to fake the physical characteristics of an individual in order to obtain a positive match in the biometric system, to consider implement anti-spoofing measures, such as liveness detection, within the system.

(c) Storage - Encrypt biometric data during storage, and separate storage of original biometric data and derived features. Must only keep biometric (and other personal) information for as long as it is necessary for its purposes.

(d) Accuracy – Must have appropriate processes in place to check the accuracy of the personal information you collect and create.

(e) Disposal - when biometric data are no longer required, ensure that the corresponding entries are permanently deleted from the system.

(f) Restrict secondary disclosures of biometric data for secondary purpose unless the secondary purpose is directly related to the primary purpose of collection and within reasonable expectations of the data subject.

Question 6

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) In your view, should the categories of personal data which can fall within the definition of "biometric data" and examples of biometric data provided above be non-exhaustive? If not, what are the other examples of personal data which should be included?

(b) Do you consider that the proposed additional measures above with respect to the processing of biometric data to be sufficient and robust? If not, what other measures should be implemented to strengthen biometric data protection?"

(c) As a data controller, to the extent that you undertake the processing of biometric personal data, do you foresee any potential challenges or difficulties in implementing such proposed additional measures? If so, what are the ways to address or mitigate such challenges or difficulties?

(d) Are there any standards or guidelines related to biometric data that are currently being imposed on data controllers within a particular sector / industry? If your answer is yes, please specify the sector / industry you are referring to along with details of such standards or guidelines.

[G] CCTV

2.33 **Background:** Given the inclusion of biometric data in the Act 709 explained above and in view of the common use of CCTV by organisations, the ADMP Guideline will also address the use of CCTV to generate biometric data and the processing of biometric data via CCTV for automated decision making and profiling purposes.

2.34 The data protection authorities of certain countries such as Singapore and UK have also issued guidance in relation to use of biometric data in security applications or relating to the use of CCTVs.

2.35 **Proposal:** It is proposed the following measures should be adopted by data controllers when deriving biometric data from CCTV or for processing biometric data using CCTV for automated decision making and profiling purposes:

(a) assessing whether the use of CCTV is appropriate in the circumstance, taking into account the reasonable expectations of the individuals whose personal data are processed and the potential impact on their rights and freedoms.

(b) only use CCTVs in locations where it achieves the specific purpose(s).

(c) placing notices at prominent locations to notify individuals that security cameras are in operation and reason of such operation (e.g. security) and signs should be more prominent and frequent in areas where people are less likely to expect that they will be monitored by a surveillance system.

(d) only use audio recording where there is an evidenced and justified need.

(e) avoid capturing footage that intrude into spaces where an individual has a reasonable expectation of privacy.

(f) manage access to the footage and database to prevent unauthorised access by implementing certain measures e.g. limiting access to storage facility or limiting number of persons who has access to the system and databases (by using password protection).

(g) implement a process to delete or overwrite the footages on a regular basis when they are not required for any investigative purposes or any other lawful purposes.

(h) provide adequate training to staff and vendors for handling access requests to data.

Question 7

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) What are your views on the proposed measures in relation to the use of CCTV as stated in the Paragraph 2.35?

(b) Are there any additional measures which should be included or removed? If so, please specify and justify.

(c) In your experience, do you foresee any potential challenges or difficulties in implementing such proposed measures? If so, what are the ways to address or mitigate such challenges or difficulties?

(d) Are there any standards or guidelines related to CCTV that are currently being imposed on data controllers within a particular sector /industry? If your answer is yes, please specify the sector /industry you are referring to along with details of such standards or guidelines.