Response to Proposed Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems

Prudential Assurance Company Singapore (Pte) Limited

Name: Jake Yeo

Email: compliance.advisory@prudential.com.sg

PACS would like to seek some guidance and clarity from PDPC in relation to the proposed advisory guidelines, specifically on the scope of AI and the consent required from individuals.

Please refer to PACS' comments to specific sections of the proposed advisory guidelines below.

4. Business Improvement Exception and Research Exception

4.1 Apart from seeking consent for the use of personal data to train an AI model, organisations may wish to consider if it is appropriate to rely on the Business Improvement or Research exceptions to consent when using personal data to develop an AI System.

4.2 Where using personal data, organisations are encouraged to undertake a data protection impact assessment to consider the effectiveness of risk mitigation and remediation measures applied to personal data.

The Business Improvement and Research Exception appear to be from the PDPA. PACS would like to clarify if FIs are required to put up an assessment to justify the exemption.

5 Application of the Business Improvement Exception

5.1 When organisations require the use of personal data in the development of the AI System, they may consider relying on the Business Improvement Exception in lieu of consent. The Business Improvement Exception caters for sharing with related companies within a group of companies, as well as interdepartmental sharing of data within a company.

5.2 Part 5 of the First Schedule and Division 2 under Part 2 of the Second Schedule to the PDPA enables organisations to use, without consent, personal data that they had collected in accordance with the PDPA, where the use of the personal data falls within the scope of any of the following business improvement purposes ("Business Improvement Exception"):

The Business Improvement and Research Exceptions appear to be from the PDPA amendments. These state that the legitimate interest exception requires an assessment before it can be applied. PACS would like to clarify if FIs are required to put up an assessment to justify the exemption during development.

5.4 To illustrate, the following are examples of purposes where the Business Improvement Exception could be relevant to AI System development:

a) Recommendation engines in social media services that offer users content more aligned to their browsing history;

b) Job assignment systems that automatically assign jobs to platform workers;

c) Internal HR systems used to recommend potential job candidates by providing a first cut in matching candidates to job vacancies; or

d) Use of AI Systems or ML models to provide new product features and functionalities to improve competitiveness of products and services.

PACS would like to clarify if the examples given also apply to production and if these use cases are good examples to apply for the legitimate interest exemption.

When using personal data for bias assessment

5.8 Personal data may need to be used to check if protected characteristics, such as race or religion, are well represented in datasets or to assess the bias of the training dataset, so that adjustments may be made for de-biasing during AI system development. In considering whether the Business Improvement Exception applies, organisations should consider the following:

a) Whether using personal data for this purpose is relevant for the effectiveness or improved quality of the AI Systems or ML models and its output;

b) Whether it is technically possible and cost-effective to use other means to debias AI Systems or ML models without using personal data; and/or

c) Common industry practices or standards on how to debias datasets used for AI Systems or ML models.

5.9 The Commission understands that generally, industry best practice is to use personal data to debias datasets used for ML model training.

PACS would like check if there is any guidance for FIs on better use of PII to infer if there any bias and whether FIs are allow to access PII to determine the extent of the bias or ignore the assumption given there is no evidence.

PACS would suggest PDPC clarify if there are methods to totally anonymize bias detection.

PACS would also like to clarify if customer consent is needed to use his/her data for model training and if so, the responsibility for managing consent lies with which stakeholder and if the wording of consents requires changes.

6 Application of the Research Exception

6.1 Division 3 under Part 2 of the Second Schedule to the PDPA allows for organisations to use personal data for a research purpose (the "Research Exception"). The Research Exception is intended to allow organisations to conduct broader research and development that may not have any immediate application on their products, services, business operations or market. This would include sharing data between unrelated companies for the purposes of jointly conducted commercial research to develop new AI Systems.

PACS would like to clarify if research mean studies that are intended for publication in the public domain and whether research with only an internal audience would be considered under this item. PACS would also suggest for PDPC to provide a definition of "research".

7 Stage of AI System Implementation: Part II : Development, testing and monitoring:

7.1 Organisations are reminded that when designing, training, testing, or monitoring AI Systems using personal data, appropriate technical, process and/or legal controls for data protection should be included. Where possible, organisations are encouraged to pseudonymise or de-identify the personal data used as a basic data protection control. In deciding what kind of controls for data protection should be implemented, as per the Advisory Guidelines on Key Concepts in the PDPA, companies should consider the following:

a) The types of disclosure/theft risks that the personal data would be subject to; and

b) The sensitivity and volume of the personal data used.

7.2 Generally, privacy controls for internal use need not be as extensive as intra-group or cross-company sharing. However, companies are still encouraged to assess the risks and implement appropriate legal, technical and process controls for such use of personal data.

PACS would like to clarify if there is guidance on how pseudo anonymizing and de identifying data can be done. Many FIs will not have much experience with this and PACS understanding that these processes can be complex and if not done properly, there will be risk not actually removing the PII exposure.

PACS would like to enquire if there are examples that FIs can follow.

7.3 In the context of developing AI Systems, organisations should practise data minimisation as good practice.

Using only personal data containing attributes required to train and improve the AI System or ML model will also reduce unnecessary data protection and cyber threat risk to the AI System.

To similarly reduce such risks, organisations should use the volume of personal data necessary to train the AI System or ML model and base this on relevant time periods and any other relevant filter e.g., market/customer segment, attributes, etc. Organisations may wish to refer to the PDPC's Guide to Data Protection Practices for ICT systems for further guidance in this area.

PACS is unable to determine what data are required during the development phase. During the development phase when preparation of multiple features, the modelling approach will identify which data are most useful. Only pertinent information will be used in production. Therefore, more data is created than needed at the start and reduce this down to the minimum.

PACS would like to clarify on the above-mentioned process is acceptable according to the guidelines.

7.4 If pseudonymisation is not possible and raw personal data has to be used e.g., facial images, organisations are reminded of their protection obligation under the PDPA.

PACS would like to clarify if the security and protection measures differ from a non-AI use case.

For example, would preparing a BI dashboard require pseudonymization and the same security and protection measures.

7.6 In addition, as per their Accountability obligation under the PDPA, organisations must ensure that their policies regarding the use of personal data in their organisations to develop AI Systems are updated and practices are established.

PACS would like to clarify if FIs need the same protections for processes using PII that use human decision making and if the policies to develop AI systems different from other systems.

Using anonymised data

7.7 Generally, organisations are encouraged to anonymise their datasets as far as possible instead of using personal data. While anonymised data is not subject to the PDPA, organisations are reminded that such data still bears risk of re-identification and disclosure, and appropriate legal, technical and process controls should be instituted when using or disclosing such data. Organisations can refer to the PDPC's Guide to Basic Anonymisation for further guidance.

PACS suggest for PDPC to provide clarity on disclosing data mentioned and examples that FIs can refer to (e.g. whether releasing information for internal use would be considered as disclosing data).

7.10 As to whether anonymisation is sufficiently robust as to reduce the risk of reidentification, this would include considerations such as:

a) Whether the process of chosen anonymisation method is reversible;

b) The extent of disclosure of the dataset and its intended recipients (e.g., internal closed-group sharing vs. cross-company sharing);

c) Whether a motivated individual can likely find means to re-identify the anonymised dataset using either publicly available information or information the organisation already has in its possession; and

d) The extent of controls the organisation has put in place, including within the AI System, to prevent re-identification of the anonymised data.

7.11 The Commission is aware that identifiability and anonymisation exists on a spectrum and is inherently context specific. It is likely that where the risk of re-identification is lower e.g., due to limited circulation or extensive controls over the anonymised data to prevent re-identification, the extent of anonymisation could be lesser to preserve the utility of the dataset.

Anonymizing data apply to all Analytics' projects. For example, a dashboard should only use PII when necessary, it should only use required data and use anonymized data. PACS would suggest PDPC to clarify whether the regulation applies to all analytics products or just AI.

<u>8 PDPA Applies to Collection and Use of Personal Data in AI Systems</u>

8.1 The previous section discussed how the PDPA applies when organisations use personal data for the development and testing of AI Systems. This section deals with how the PDPA applies when organisations deploy AI Systems in their products or services that collect and use personal data.

8.2 When organisations deploy AI Systems to provide new functionalities or enhance product features by collecting and/or processing personal data, they should be mindful of the following PDPA obligations: Consent and Notification as well as Accountability.

AI systems developed are done with the intention of deploying the system to production. The guidelines for deployment have more rigor than those for development. PACS would suggest PDPC to clarify if customer consent is required during development (e.g. model training before deployment).

<u>9 Consent and Notification Obligations</u>

9.1 When AI Systems are deployed to end users, personal data may be collected and/or processed by the AI System to provide the recommendation, prediction or decision. Unless deemed consent or exceptions to the consent obligation apply (e.g., legitimate interests exception), pursuant to Section 13 of the PDPA, consent will be required for such collection and use of personal data. Section 13 of the PDPA provides that organisations are allowed to collect, use, or disclose an individual's personal data if the individual gives his consent for the collection, use or disclosure of his personal data. This is referred to as the Consent obligation.

Currently FIs have existing data collection processes that were collecting data for non AI systems. PACS would like to check with PDPC if FIs are allowed to infuse AI into these processes and any changes is required.

10 The Accountability Obligation

10.1 The Accountability Obligation under the PDPA refers to how an organisation discharges its responsibility for personal data which it has collected or obtained for processing, or which it has control over. Sections 11 and 12 of the PDPA detail the various actions to be carried out by organisations in fulfilment of this obligation.

10.2 Amongst other things, Section 12 of the PDPA requires organisations to develop policies and practices to meet its obligations under the PDPA. Written policies and documentation of processes enable organisations to show that their internal governance and supervision structures, and operational practices ensure that personal data is used responsibly, either in line with purposes that individuals have been notified of and consented to or for legitimate purposes that a reasonable person would consider appropriate in the circumstances.

10.3 Organisations that make use of AI Systems should be transparent and include relevant practices and safeguards to achieve fairness and reasonableness in their written policies.14 The level of detail to be provided under the Accountability Obligation should also be proportionate to the risks present in each use-case (e.g., taking into account potential harm to the individual and the level of autonomy of the AI System).

10.4 Section 12(d) requires organisations to make information about such policies and practices available to individuals upon request. The raison d'etre for such external communications with consumers is to help organisations build trust with data subjects by demonstrating accountability in their compliance with the PDPA. Hence, organisations should consider pre-emptively making such written policies available through their website, and not only upon request of individuals. Organisations should also consider making such written policies available in the form of short policy statements that provide information to consumers simply, clearly, and concisely. Additionally, developing industry best practices, such as model cards and system cards, can also form part of an organisation's written policies.

10.5 Written policies can house the more detailed information that organisations ought to provide to obtain meaningful consent. This is discussed in the preceding section concerning the layering of information when meeting the Consent and Notification Obligations. Where organisations have relied on exceptions to the requirement of consent, such as Business Improvement and Research Exceptions, written policies can also provide information about the practices and safeguards that were adopted to protect the interests of individuals.

PACS would suggest PDPC to clarify if the new provision applies for all data systems and not solely for AI.

10.7 Not all these measures are required. Organisations using personal data for model development and testing, and in deployed AI Systems, should consider adopting measures that a reasonable person would consider appropriate in the circumstances. Having done so, organisations are encouraged to consider providing sufficient information about such measures to build consumer trust and confidence.

PACS would also suggest for PDPC to provide more clarity on "reasonable" as AI is yet to have common standards and there are big differences in AI risk appetite across various nations (comparing the EU's AI Act to other nations, "reasonable" is subjective).

PACS would suggest PDPC to clarify if these guidelines apply only to AI/ML or more broadly to any analytics service or product and the requirement to ask customer for consent to use their data for AI but not have to ask if is for basic statistics or rule based engines.