Artificial Intelligence:
Model Personal Data Protection Framework

that organisations should incorporate into their business process when they procure, implement and use AI

Provide feedback for adjustment

ESTABLISH
AI Strategy and Governance

CONDUCT
Risk Assessment and Human Oversight

EXECUTE
Customisation of AI Models and Implementation and Management of AI Systems

FOSTER
Communication and Engagement with Stakeholders

Re-assess risks when there are significant changes

Fine-tune AI systems to address stakeholders' concerns

ESTABLISH - AI Strategy and Governance

7 Steps in AI Procurement

1. Sourcing AI solutions
2. Picking the appropriate AI solution
3. Collecting and preparing data
4. Customising AI model for particular purpose
5. Testing, evaluating and validating AI model
6. Testing and auditing system and components for security and privacy risks
7. Integrating AI solution into organisation's system

9 Governance Considerations

- Purposes of using AI
- Privacy and security obligations and ethical requirements
- International technical and governance standards
- Criteria and procedures for reviewing AI solutions
- Data processor agreements
- Policy on handling output generated by the AI system
- Plan for continuously scrutinising changing landscape
- Plan for monitoring, managing and maintaining AI solution
- Evaluation of AI suppliers

Risk-based Approach to Human Oversight

CONDUCT
Risk Assessment and Human Oversight

Lower   ***Risk level of AI system***   *Higher*

Human-out-of-the-loop
AI makes decisions without human intervention

Human-in-command
Human actors oversee the operation of AI and intervene whenever necessary

Human-in-the-loop
Human actors retain control in the decision-making process

EXECUTE
Customisation of AI Models and Implementation and Management of AI Systems

Process	Selected Recommendations
Data Preparation	Ensure compliance with privacy law • Manage data quality • Minimise the amount of personal data involved • Document data handling
Customisation and Implementation of AI	Conduct rigorous testing and validation of reliability, robustness and fairness • Consider compliance issues based on the hosting of AI solution ('on-premise' or on a third party cloud) prior to integration • Ensure system security and data security
Management and Continuous Monitoring of AI	Maintain proper documentation • Conduct periodic audits • Establish an AI Incident Response Plan • Consider incorporating review mechanisms as risk factors evolve

---

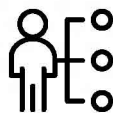**FOSTER**
Communication and Engagement with Stakeholders

Stakeholders

Internal Staff   AI Suppliers   Customers   Regulators

Disclaimer

The information and suggestions provided in this publication are for general reference only. They do not serve as an exhaustive guide to the application of the law and do not constitute legal or other professional advice. The Privacy Commissioner makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information and suggestions set out in this publication. The information and suggestions provided will not affect the functions and powers conferred upon the Privacy Commissioner under the Personal Data (Privacy) Ordinance.

June 2024