Artificial Intelligence: Model Personal Data Protection Framework that organisations should incorporate into their business process when they procure, implement and use AI.

1. **EstABLish** - AI Strategy and Governance
   - 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

2. **Conduct** - Risk Assessment and Human Oversight
   - Re-assess risks when there are significant changes

3. **Execute** - Customisation of AI Models and Implementation and Management of AI Systems
   - Fine-tune AI systems to address stakeholders' concerns

4. **Foster** - Communication and Engagement with Stakeholders

**7 Steps in AI Procurement**

**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

Supporting Organizations:
- 中華人民共和國香港特別行政區政府
  政府資訊科技總監辦公室
  Office of the Government Chief Information Officer
  The Government of the Hong Kong Special Administrative Region of the People's Republic of China
- Hong Kong Applied Science and Technology Research Institute

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong
Risk-based Approach to Human Oversight

Risk Assessment and Human Oversight

**CONDUCT**

- **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 of AI Systems

**Process**

- **Data Preparation**
  - Ensure compliance with privacy law
  - Minimise the amount of personal data involved

- **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
  - Establish an AI Incident Response Plan

**Selected Recommendations**

- Manage data quality
- Document data handling
- Conduct periodic audits
- Consider incorporating review mechanisms as risk factors evolve

**STAKEHOLDERS**

- **Internal Staff**
- **AI Suppliers**
- **Customers**
- **Regulators**

**FOSTER**

Communication and Engagement with Stakeholders

**PCPD Website:** pcpd.org.hk

**Disclaimer**

This publication is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence. In essence, you are free to share and adapt this publication, as long as you attribute the work to the Office of the Privacy Commissioner for Personal Data, Hong Kong. For details, please visit creativecommons.org/licenses/by/4.0.

Tel : 2627 2627
Fax : 2677 7026
Address : Unit 1303, 13/F., Dah Sing Financial Centre, 248 Queen’s Road East, Wanchai, Hong Kong
E-mail : communications@pcpd.org.hk

June 2024