June 2024 legal and regulatory update

Appendix II Summary of PCPD recommendations

(Note: page references refer to PCPD full document)

I. AI STRATEGY AND GOVERNANCE (P.11)

- **AI strategy**
  - **Key principle: accountability**
  - Demonstrate **commitment of top management** to **ethical and responsible** procurement, implementation and use of AI
  - Provide **directions on**
    - **purposes** for which AI solutions may be procured
    - how AI systems should be **implemented** and **used**
  - **Elements**
    - e.g. define the functions that AI systems would serve; set ethical principles; determine unacceptable uses
- **Governance considerations for procuring AI solutions**
  - Generally involves engaging third parties to **customise** AI systems or buying **off-the-shelf** systems
  - Governance considerations (P.13)
    - e.g. purposes of using AI; key privacy and security obligations and ethical requirements; international technical and governance standards
- **Governance structure**
  - **Key principles: accountability/human oversight**
  - Establish an **internal governance structure** with sufficient resources, expertise and authority
  - **AI governance committee**
    - **report to board** and **oversee whole life cycle** of AI solutions from procurement, implementation, and use to termination
    - oversight **across business**, not to be constrained by division *(e.g. risk and compliance)*
    - participated by **senior management** and **interdisciplinary collaboration**
    - **led** by a **C-level** executive
    - examples of roles and responsibilities (P.19)

Copyright © 2024 Practising Governance

- **Training and awareness raising**
  - **Key principle: accountability**
  - E.g. for AI system users: compliance with data protection laws/regulations/internal policies; cybersecurity risks; general AI technology
  - Training for other personnel, e.g. legal and compliance professionals (P.21)
  - Roles of **human reviewers** (P.21)

II. RISK ASSESSMENT AND HUMAN OVERSIGHT (P.23)

- **General: a risk-based approach**
  - In the **procurement, use and management** of AI systems
  - **Comprehensive risk assessment**
    - **identify**, **analyse** and **evaluate** risks *(including privacy risks)*
  - **Risk management system** formulated/implemented/documented/maintained
    - **throughout entire life cycle** of system
  - **Cross-functional team** to conduct risk assessment
    - during **procurement** process or **significant updates**
  - All risks assessment be properly **documented**
- **Risk factors**
  - **Key principles: beneficial AI/data privacy/fairness**
  - **Key factors** considered in **risk assessment**
    - e.g. allowable uses of data (**DPP3**)

      (Under DPP3, personal data must not be used for new purposes without the prescribed consent of data subjects)
    - e.g. volume of personal data (**DPP1**)

      (Under DPP1, amount of personal data to be collected shall be adequate but not excessive)
- **Determining level of human oversight**
  - **Key principle: human oversight**
  - **Risk-based** approach: type/extent of **risk mitigation** measures **proportionate** to risks
  - **Human oversight** is a key measure for mitigating risks
  - Examples of AI use cases that may incur higher risk (P.29)
- **Risk mitigation trade-offs** (P.30)

Copyright © 2024 Practising Governance

III. CUSTOMISATION OF AI MODELS AND IMPLEMENTATION AND MANAGEMENT OF AI SYSTEMS (P.32)

- **Data preparation for customisation and use of AI**
  - **Key principles: data privacy/fairness**
  - 4 aspects of **data preparation**
    - compliance with requirements of PDPO
    - minimisation of personal data involved in customisation and use of AI
    - management of data for customising and using AI
    - proper documentation of handling of data
- **Customisation and implementation of AI solutions**
  - **Key principles: transparency and interpretability/reliability, robustness and security**
  - **Rigorous testing** and **validation** in **proportion to risks** involved
  - Recommended measures (P.38)
- **Management and continuous monitoring of AI systems**
  - **Key principles: reliability, robustness and security/human oversight**
  - **Monitored** and **reviewed continuously**
    - risk factors may change
  - Consider establishing an **AI incident response plan** *(P.45: detailed elements)*

IV. COMMUNICATION AND ENGAGEMENT WITH STAKEHOLDERS (P.47)

- **Key principle: transparency and interpretability**
- **Information provision**
  - Communicate and engage effectively and regularly with stakeholders
    - in particular **internal staff**, **AI suppliers**, individual **customers** and **regulators**
  - **Level of transparency** will **vary** depending on stakeholders
  - Effective communication is essential to **building trust**
- **Data subject rights and feedback**
- **Explainable AI**
  - Key to **building trust** with stakeholders
  - Making the decisions and output of AI explainable

Copyright © 2024 Practising Governance

- **Language and manner**
    - Plain language, clear and understandable to lay persons

Copyright © 2024 Practising Governance