BCLP. Client Intelligent

Insights

HONG KONG ISSUES GUIDANCE ON THE USE OF AI

Nov 18, 2021

SUMMARY

Hong Kong now has its own set of recommended best practices for the development and use of AI published in a guidance note issued by the PCPD. Businesses which intend to or have begun to use AI in their operations are advised to consider the risk levels of their respective AI systems and implement the suggested measures for better protection of individual consumers.

An artificial intelligence ("AI") system is a machine-based system which makes predictions, recommendations for decisions influencing real or virtual environments, based on a given set of human-defined objectives. The potential social and economic benefits of AI are significant. Healthy use of AI can drive innovation and improve efficiency in a wide range of fields.

However, given the nature of what an AI system does, it also comes with potential risks which no business should ignore. AI systems often involve the profiling of individuals and the making of automated decisions which have real impact on human beings, posing risks to data privacy and other human rights.

Against this background, calls for accountable and ethical use of AI have been on the rise in recent years.

In October 2018, the Global Privacy Assembly ("GPA")[1] adopted a "Declaration on Ethics and Data Protection in Artificial Intelligence", endorsing six guiding principles to preserve human rights in the development of AI. Two years later, the GPA adopted a resolution sponsored by the Office of the Privacy Commissioner for Personal Data ("PCPD") of Hong Kong to encourage greater accountability in the development and use of AI. Various countries and international organisations have published their respective guidance notes to encourage organisations to embrace good data ethics in their operation and use of AI.

The PCPD published its "Guidance on the Ethical Development and Use of Artificial Intelligence" (the "Guidance") in August 2021. This blog post summarises the key highlights from the Guidance.

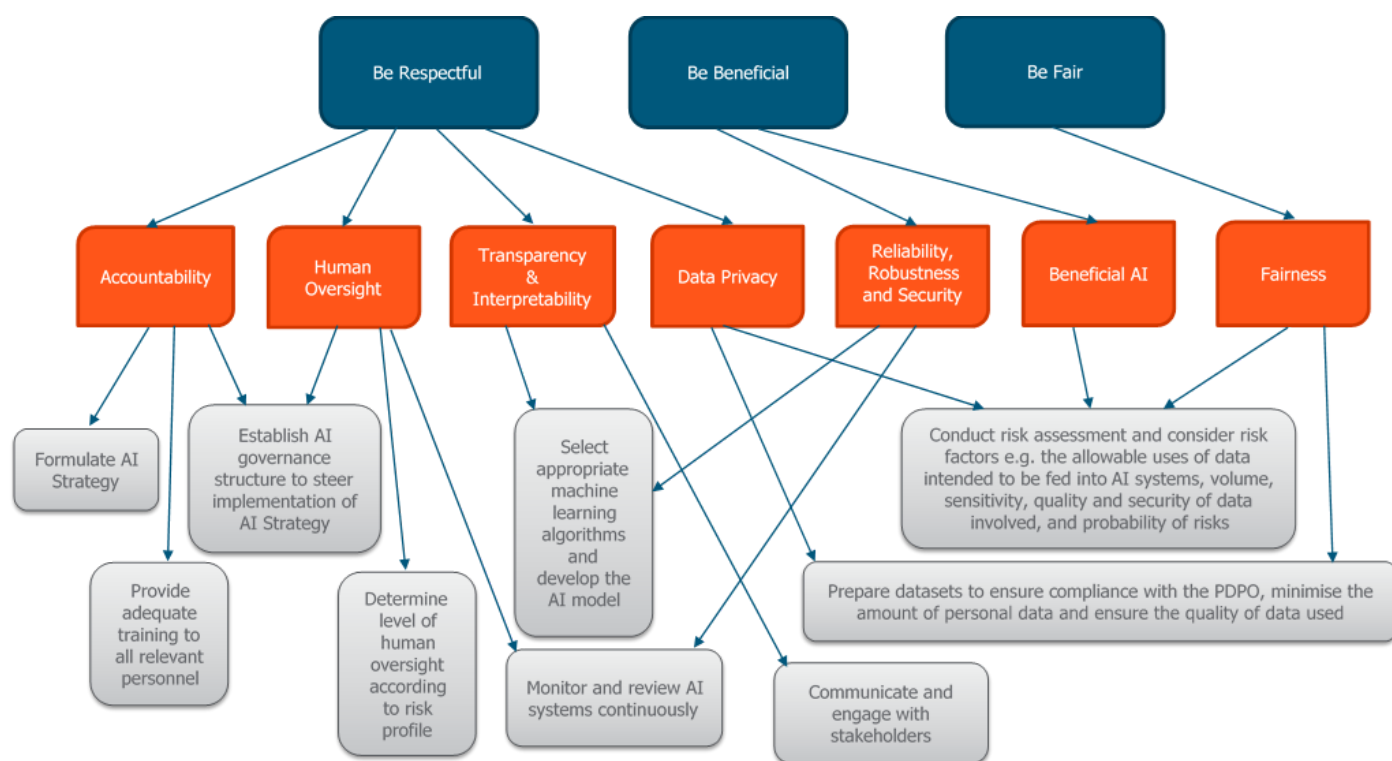## FROM HIGH-LEVEL VALUES TO GROUND-LEVEL PRACTICES

The Guidance sets out three broad "Data Stewardship Values" which transform into various ethical principles and specific practical guidance.

Three Data Stewardship Values were put forward by the PCPD in October 2018 in the Ethical Accountability Framework for Hong Kong. Businesses should recognise and embrace these core ethical values. These values should define how businesses carry out their activities and achieve their missions or visions.

The three Data Stewardship Values entail the following:

- Be respectful to the dignity, autonomy, rights, interests and reasonable expectations of individuals;

- Be beneficial to stakeholders and to the wider community with the use of AI; and

- Be fair in both processes and the results:

- Make sure that decisions are made reasonably, without unjust bias or unlawful discrimination.

- Accessible and effective avenues need to be established for individuals to seek redress for unfair treatments.

- Like people should be treated alike. Differential treatments need to be justifiable with sound reasons.

These three core values are linked to some commonly accepted principles such as accountability, transparency, fairness, data privacy and human oversight found also in guidance notes published in other countries or by international organisations. These principles then have been fleshed out and developed into recommended ground-level practices by the PCPD:

Be Respectful | **Be Beneficial** | **Be Fair**

Accountability | Human Oversight | Transparency & Interpretability | Data Privacy | Reliability, Robustness and Security | Beneficial AI | Fairness

- Formulate AI Strategy
- Establish AI governance structure to steer implementation of AI Strategy
- Provide adequate training to all relevant personnel
- Determine level of human oversight according to risk profile
- Select appropriate machine learning algorithms and develop the AI model
- Monitor and review AI systems continuously
- Conduct risk assessment and consider risk factors e.g. the allowable uses of data intended to be fed into AI systems, volume, sensitivity, quality and security of data involved, and probability of risks
- Prepare datasets to ensure compliance with the PDPO, minimise the amount of personal data and ensure the quality of data used
- Communicate and engage with stakeholders

AI STRATEGY AND GOVERNANCE

The Guidance recommends that organisations that use or intend to use AI technologies should formulate an AI strategy. Internal policies and procedures specific to the ethical design, development and use of AI should be set up.

First and foremost, in order to steer the development and use of AI, organisations should establish an internal governance structure which comprises both an organisational-level AI strategy and an AI governance committee (or a similar body). The AI governance should oversee the entire life cycle of the AI system, from development, use to termination. It should comprise a Chief-level executive to oversee the AI operation, as well as members from different disciplines and departments to collaborate in the development and use of AI.

Internal governance policies should spell out the clear roles and responsibilities for personnel involved in the use and development of AI. Adequate financial and human resources also should be set aside for the development and implementation of AI systems. Since human involvement is key, the Guidance also recommends providing relevant training to and arrange regular awareness-raising exercises for all personnel involved in the development and use of AI.

RISK ASSESSMENT AND HUMAN OVERSIGHT

The Guidance stresses the element of human oversight and the fact that human actors ultimately should be held accountable for the use of and the decisions made by AI. An appropriate level of human oversight and supervision, which corresponds with the level of risk, should be put in place.

An AI system that is likely to cause a significant impact on stakeholders is considered to be of high risk. An AI system with higher risk profile require a higher level of human oversight.

In order to determine risk level, risk assessments which take into account personal data privacy risks and other ethical impact of the prospective AI system should be conducted before the development and use of AI. Risk assessment results should be reviewed and endorsed by the organisation's AI governance committee or body, which then should determine and put in place an appropriate level of human oversight and other mitigation measures for the AI system.

DEVELOPMENT OF AI MODELS AND MANAGEMENT OF AI SYSTEMS

To better protect data privacy, the Guidance recommends that organisations should take steps to prepare datasets which are to be fed to the AI systems. Where possible, organisations should consider using anonymised or synthetic data which carries no personal data risk. The Guidance further recommends that organisations should minimise the amount of personal data used by collecting only the data that is relevant to the particular purposes of the AI in question, and strip away individual traits or characteristics which are irrelevant to the purposes concerned.

The quality of data used should be monitored and managed. "Quality data" should be reliable, accurate, complete, relevant, consistent, properly sourced and without unjust bias or unlawful discrimination. Organisations should take appropriate measures to ensure the quality of data and compliance with PDPO requirements.

Once datasets are prepared, organisations will have to evaluate, select and apply (or design) appropriate machine learning algorithms to analyse the training data. Mitigation measures which reduce the risk of malicious input and rigorous testing of the AI models are recommended so as to improve the AI system. It also is important to have mechanisms which allow for human intervention and fallback solutions to kick in when necessary.

AI systems run by machines always have a chance (however slight) of mal-functioning or failing. It therefore is important for them to be subject to continuous review and monitoring by human beings. The approach to such human monitor and review again should vary depending upon the risk level. Measures proposed in the Guidance include keeping proper documentation, implementing security measures throughout the AI system life cycle, re-assessing risks and re-training AI models from time to time, and establishing feedback channels for users of the AI system.

Taking one step back from the AI systems, organisations also are encouraged to conduct regular internal audit and evaluation of the wider technological landscape to identify gaps or deficiencies in the existing technological ecosystem.

COMMUNICATION AND ENGAGEMENT WITH STAKEHOLDERS

Organisations which serve individual consumers using AI should ensure that the use of AI is communicated to the consumers in a clear and prominent manner and using layman terms. Many of the recommendations set out in the Guidance mirror the data protection principles in place for the collection and use of personal data. For example, consumers should be informed of the purposes, benefits and effects of using the particular AI system. Consumers also should be allowed to correct any inaccuracies, provide feedback, seek explanation, request human intervention and opt out from the use of AI where possible. Where appropriate, results of risk assessments and re-assessments also should be disclosed to consumers.

CONCLUDING REMARKS

The Guidance encompasses detailed and practical guidelines which have been developed after having considered relevant international agreement and practices. It provides useful guidance to businesses which intend to jump on the bandwagon of the AI trend or which are seeking to ensure their current AI systems are complaint with best practices endorsed by the Hong Kong government.

Although compliance with the Guidance is not mandatory, prudent businesses and organisations should implement the recommended measures set out in the Guidance to the extent possible, especially if their use or intended use of AI comes with high data or security risk.

The topic of AI has attracted more and more attention in the international arena in the past few years. General artificial intelligence bills or resolutions have been introduced and enacted in a number of states in the US in 2021. In April 2021, the European Commission proposed to regulate AI by legislative means. In addition to implementing the recommended measures, multi-national companies should keep a close watch on the development of the law in this area in their relevant jurisdictions.

[1] The GPA is a leading international forum for over 130 data protection regulators from around the globe to discuss and exchange views on privacy issues and the latest international developments.

RELATED CAPABILITIES

- Data Privacy & Security
- Corporate

MEET THE TEAM

Glenn Haley

Hong Kong SAR

glenn.haley@bclplaw.com
+852 3143 8450