Mastering Big Data and Privacy

DR G

1 May 2023

A bit of recent history and sharing

From MIT's Professor Alex Pentland.

Session Agenda

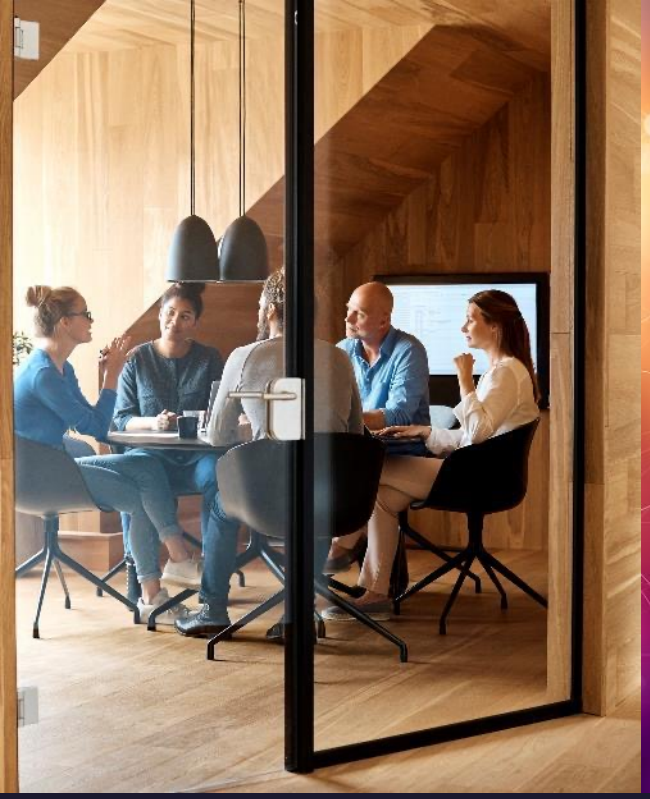
EU's GDPR

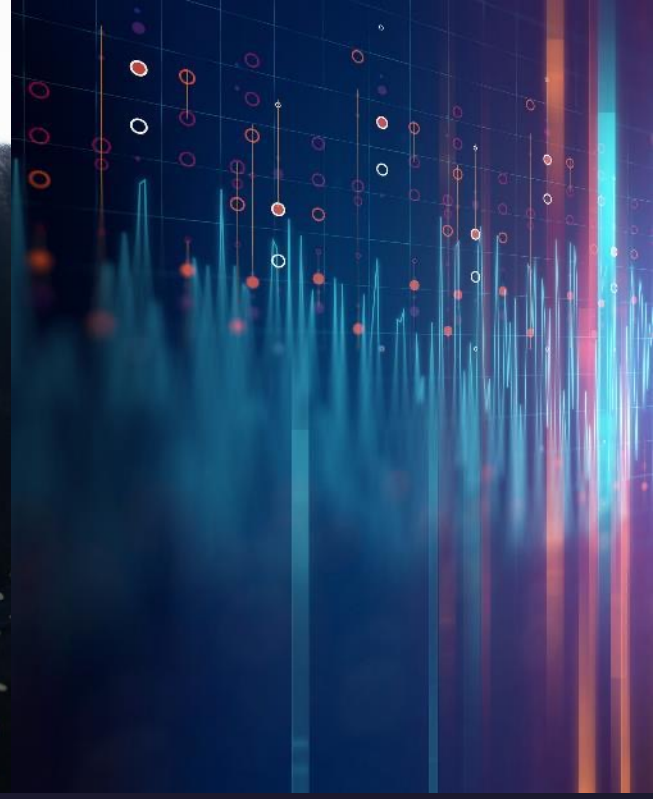
China's PIPL

Hong Kong's PDPO

US's PPDSA

Implications for Your New Company and Data Landscape



EU's General Protection Data Regulation (GDPR)

- A landmark piece of legislation that affects companies worldwide when doing business with EU citizenship.
- Became the basis of many national laws on privacy.

1. GDPR is a **comprehensive** **privacy** regulation imposed by the European Union (EU) to protect the privacy rights of EU citizens.

2. To comply with GDPR, businesses must ensure that they have **appropriate systems and processes in place to collect, manage, use, and protect personal data. Businesses must also obtain consent** from individuals to collect, use, and share their personal data and inform them about the type of data collected and how it will be used.

3. GDPR gives individuals several rights related to their personal data, such as the right to access, correct, and **delete their personal data**. Businesses must respect these rights and respond promptly to individuals' requests related to their personal data.

4. GDPR requires businesses to report data breaches that affect EU citizens to the relevant authorities within **72 hours of discovery**. Businesses must also inform affected individuals about data breaches that could result in a high risk to their privacy rights.

5. Penalties for non-compliance: Businesses that fail to comply with GDPR's rules can face significant penalties, including fines of up to **4% of their annual global turnover or €20 million**, whichever is greater. Businesses must take GDPR compliance seriously to avoid these penalties and protect individuals' privacy rights.

China's Privacy Law and X-Border Data Protection or PIPL

Relevant for us is X-Border Transfer of Data

- **China's Personal Information Protection Law (PIPL**) is a comprehensive national law that aims to regulate the collection, use, and sharing of personal information. Came into effect on November 1, 2021.The law applies to companies and organizations that process the personal information of **Chinese citizens**, **regardless of whether they are located in China or overseas**. It covers the entire data life cycle, from the collection, processing, storage, and use of personal information to its transfer and sharing.

- Under the PIPL, individuals have certain rights with respect to their personal information, such as the right to know how their data is being used, the right to access, review, modify, and **delete** their personal information, and the right to object to the processing of their personal information in certain circumstances.

- The PIPL also imposes specific obligations on data controllers, including obtaining individual consent before collecting and processing personal data, and adopting reasonable and necessary measures to protect the security and confidentiality of personal information. Additionally, the law restricts the transfer of personal data outside of China unless certain criteria are met, such as obtaining consent from individuals or obtaining an adequacy decision from the Chinese government.

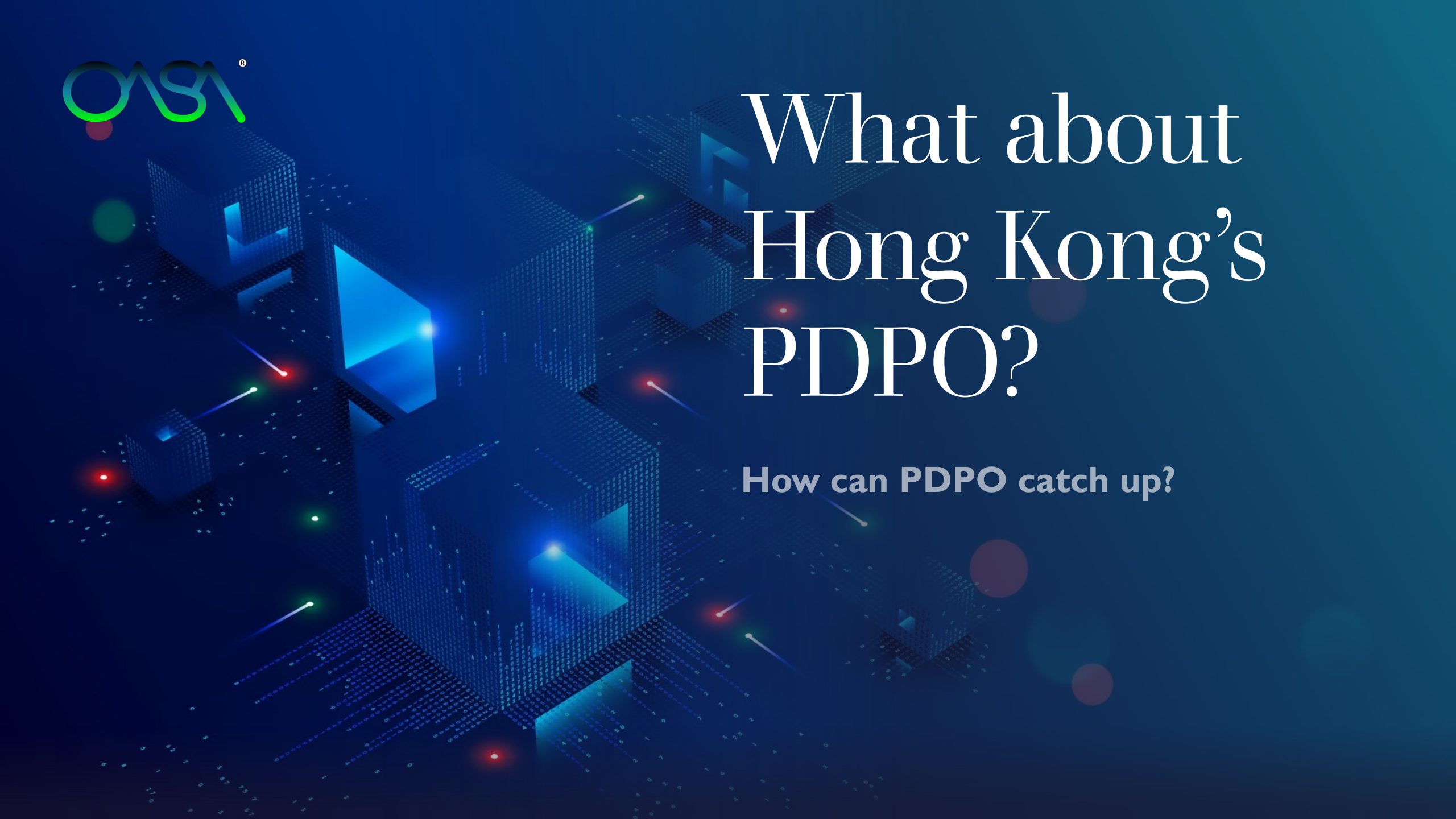
- The PIPL **sets out penalties for non-compliance, including substantial fines for companies and potential criminal liability for individuals in some cases**. The law is considered to be one of the world's most comprehensive privacy laws, and is expected to have a significant impact on businesses operating in China, as well as those that process the personal information of Chinese citizens.

- **China's cross-border data transfer law** refers to the regulations governing the transfer of personal information by operators of **critical information infrastructure (CII)** and other important data outside of mainland China. The rules are laid out in the Cybersecurity and Data Security Law, which came into effect on **September 1, 2021.**

- Under the Cybersecurity Law, critical **infrastructure operators and other key data controllers must conduct a security assessment before transferring important data to a foreign country**. Such assessments involve evaluating the risks associated with data transfers, including whether the destination country has appropriate data protection measures and whether the data being transferred involves sensitive national security or industry information.It requires that **critical information infrastructure operators conduct a security assessment** to determine if they are allowed to transfer personal information or other important data overseas.

- **In addition, operators must also satisfy the following requirements prior to transferring personal information or other important data overseas:**1. Obtain the individual's consent for the overseas transfer; 2. Sign a cross-border data transfer agreement with the recipient. 3. The recipient must be certified by a regulator or meet other conditions for transfer; 4. There must be no harm caused to the rights and interests of the individual.

- The penalties for non-compliance with China's cross-border data transfer rules can be severe. **Directors are held personally liable.**



What about Hong Kong's PDPO?

How can PDPO catch up?

- 1. **Weak Enforcement:** The current PDPO lacks strong enforcement mechanisms and penalties, which may undermine the effectiveness of the law in protecting personal data privacy.
- 2. **Limited Scope:** The PDPO only applies to personal data held by a data user (i.e., the "controller") in relation to commercial transactions. It does not extend to the public sector or to data processing activities that are not related to commercial transactions.
- 3. **Outdated Language**: The language used in the PDPO is outdated and may no longer reflect the nuances of modern data processing practices. For example, the law does not specifically address issues related to cloud computing, Internet of Things (IoT), or artificial intelligence (AI)
- 4. **Lack of Data Portability**: The PDPO does not provide for data portability, which means that individuals cannot easily transfer their personal data from one organization to another.
- 5. **Inadequate Data Protection**: The measures required to protect personal data under the PDPO may be insufficient, and it does not specify technical or organizational measures that data controllers/operators are required to implement to ensure data protection.
- 6. **Limited Rights**: The rights of data subjects under the PDPO are more limited than in some other jurisdictions. For example, there is no right to be forgotten or right to object to automated decision-making.

US's National Strategy to Advance Privacy-Perserving Data Sharing and Analytics (PPDSA)

Released by the White House in March 2023, their national strategy establishes four guiding principles in developing PPDSA technologies to maximize their benefits in an equitable manner, promote trust, and mitigate risks:

1) Crafting PPDSA technologies that protect civil rights.
2) Promoting innovation alongside equity.
3) Building technologies with accountability mechanisms.
4) Minimizing exposure of vulnerable groups.

The State of California currently beats all other states in scope, penalty, and comprehensiveness. Called the Consumer Privacy Act or CCPA. (Right to opt out of sales of personal info, much stronger protection of personal health data).

Source: Victoria Beckman, 2023

16 Recommendations:

- Establish a steering group to support PPDSA guiding principles and strategic priorities.
  - Clarify the use of PPDSA technologies within the statutory and regulatory environments.
  - Develop capabilities and procedures to mitigate privacy incidents.
  - Develop a holistic scientific understanding of privacy threats, cyberattacks, and harms.
  - Invest in foundational and use-inspired R&D.
  - Expand and promote interdisciplinary R&D at the intersection of science, technology, policy and law.
  - Promote applied and translational research and systems development.
  - Pilot implementation activities within the federal government.
  - Establish technical standards for PPDSA technologies.
  - Accelerate efforts to develop standardized taxonomies, tool repositories, measurement methods, benchmarking and testbeds.
  - Improve usability and inclusiveness of PPDSA solutions.
  - Expand institutional expertise in PPDSA technologies.
  - Educate and train participants on the appropriate use and deployment of PPDSA technologies.
  - Expand privacy curricula in academia.
  - Foster bilateral and multilateral engagements related to a PPDSA ecosystem.
  - Explore the role of PPDSA technologies to enable cross-border collaboration.

The way to get started is to quit talking and begin doing.

Walt Disney

The OASA Way

HAVE DONE

- Installed a powerful Governance Architecture
- Set in a Code of Conduct
- Established a Data Protection Officer

WILL BE DOING

- Update our files and email addresses.
- Partner with eBRAM, ASTRI, HKPC and other institutions to strengthen the processes and procedures for remedial actions.
- Strengthen the roles and authority of the DP Officer

Summary

Data Privacy is one of the most important topics to set as foundation for your new company. Start early.

Thank You

Dr G

drg@oasahk.org

www.oasahk.org