


## Data Governance for the Digital Economy

**Ir. Allen Yeung, JP**

**Founding Chairman, Institute of Big Data Governance**

Oct 08, 2021

- The value of data lies in its secure and efficient access, exchange, and processing
- Data aggregation will naturally attract capital, talent, and technology



COVID-19 has accelerated the digitalisation of the global economy. Between 2020 and 2023, companies are projected to spend \$6.8 trillion on digital transformation, **while 60% of global GDP will be digitised by the end of 2021**



**TRADE IN THE DIGITAL ECONOMY**  
A PRIMER ON GLOBAL DATA FLOWS FOR POLICYMAKERS  
Prepared by the ICC Commission on Trade and Investment Policy and the ICC Commission on the Digital Economy

*Global flows have raised world GDP by at least 10 percent; this value totalled \$7.8 trillion in 2014 alone. Data flows now account for a larger share of this impact than global trade in goods. **Global flows generate economic growth primarily by raising productivity, and countries benefit from both inflows and outflows.***

- 國家的《第十四個五年規劃和2035年遠景目標綱要》指出「加強粵港澳產學研協同發展，完善廣深港、廣珠澳科技創新走廊和深港河套、粵澳橫琴科技創新極點“兩廊兩點”架構體系，推進綜合性國家科學中心建設，便利創新要素跨境流動」的要求。
- 中共中央辦公廳、國務院辦公廳印發了《深圳建設中國特色社會主義先行示範區綜合改革試點實施方案（2020 - 2025年）》（實施方案），「加快培育數據要素市場。率先完善數據產權制度，探索數據產權保護和利用新機制，建立數據隱私保護制度。試點推進政府數據開放共享。支持建設粵港澳大灣區數據平臺，研究論證設立數據交易市場或依托現有交易場所開展數據交易。開展數據生產要素統計核算試點」。

➤ Cybersecurity Law:

- Legislated on 7 Nov 2016
- “Security assessments and approval from industry regulatory bodies are required for data transfer outside mainland China.”
- Chinese companies seeking to list overseas will be subjected to regulatory screening by gov authorities if they have 1 million or more users with registered personal information
  - Didi cybersecurity review expected to set precedent for future ‘national security’ probes into data collection
- Tesla Inc. has pledged to store any data it collects in mainland China in the country, a month after its cars were banned from military complexes and housing compounds because of concerns about sensitive information being collected by cameras built into the vehicles.

- The General Data Protection Regulation (GDPR) came into force on 25 May 2018.
- The new rules apply to any company or organization that handles personal data belonging to individuals within the EU — in relation either to offering goods and services, or to monitoring the behavior of individuals within the EU.
- The definition of processing is designed to cover practically every type of data usage and includes collection, storage, retrieval, alteration, storage and destruction.
- EU's data protection authorities can impose fines of up to up to €20 million, or 4 percent of worldwide turnover for the preceding financial year—whichever is higher

- Legislated on August 20, 2021, and will take effect on November 1, 2021.
- Key Points:
  - Extraterritorial effect: PIPL applies to those who process personal information about Chinese individuals inside China as well as those who process personal information about Chinese individuals outside China.
  - Legal basis: PIPL expands the legal bases for processing personal information to seven, including where it is necessary for the performance of a contract with the individual.
  - Data transfer restrictions and localization requirements: Critical information infrastructure operators (CIIOs) and those who exceed the threshold of personal information processed set by the Cyberspace Administration of China (CAC) must store personal information in China unless they pass a CAC security assessment. PIPL also imposes more stringent requirements on cross-border data transfers, e.g., consent of the individual is always required.
- Processing activities outside China: PIPL applies to the processing of personal information carried out outside China, where the purpose is (i) to provide products or services to natural persons in China; or (ii) to analyze or assess the activities of natural persons in China.
- Fines:
  - Those who violate PIPL may face fines of up to 5% of annual revenue of the previous year or CNY50 million

- Legislated on June 10, 2021, which will take effect on September 1, 2021.
- The Data Security Law will enhance an increasingly comprehensive legal framework for information and data security in the PRC.
- Key Points:
  - Applies to a wide range of data and data activities, with extraterritorial jurisdiction
  - Refines regulations on “important data” and emphasizes protection of “core state data”
- Fines:
  - CNY2 million per case and/or revocation of business licenses or demands to close down businesses
  - CNY10 million per case and/or revocation of business licenses or demands to close down businesses, and bear criminal responsibilities (if applicable) for violating the core state data management system or harm state sovereignty, national security



## 1. Amazon — €746 million (\$877 million)

- It's tempting to force users to “agree” to cookies—or make opting out of cookies difficult—to collect as much personal data as possible.

## 2. Google – €50 million (\$56.6 million)

- The case related to how Google provided privacy notice to its users—and how the company requested their consent for personalized advertising and other types of data processing.
- **How the fine could have been avoided:** Google should have provided more information to users in consent policies and granted them more control over how their personal data is processed.

## 3. British Airways – €22 million (\$26 million)

- In 2018, British Airways's systems were compromised. The breach affected 400,000 customers and hackers got their hands on log-in details, payment card information, and travelers' names and addresses.
- **How the fine could have been avoided:** According to the ICO, the attack was preventable, but BA didn't have sufficient security measures in place to protect their systems, networks, and data. In fact, it seems BA didn't even have basics like multi-factor authentication in place at the time of the breach.
- Going forward, the airline should take a security-first approach, invest in security solutions, and ensure they have strict data privacy policies and procedures in place.



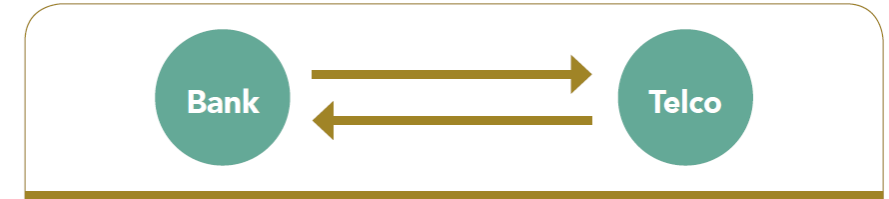
# TRUSTED DATA SHARING FRAMEWORK

**SG:D**  
EMPOWERING POSSIBILITIES

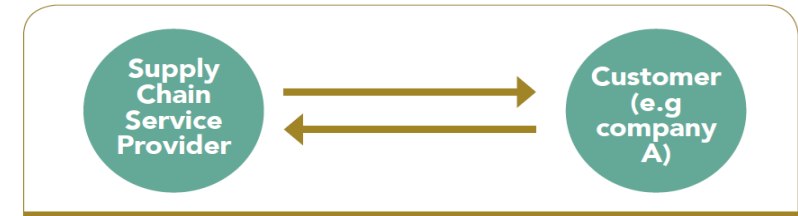
**IM** INFOCOMM  
MEDIA  
DEVELOPMENT  
AUTHORITY

**pdpc** PERSONAL DATA  
PROTECTION COMMISSION  
SINGAPORE

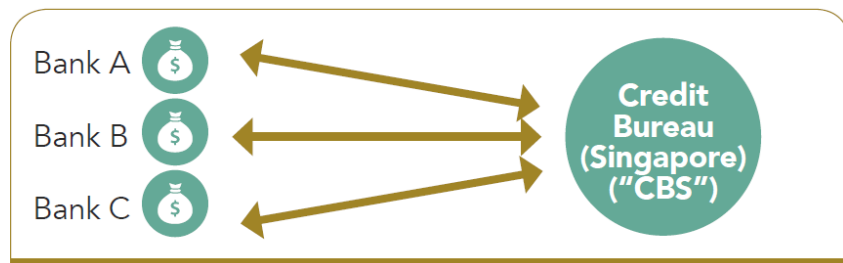
**a** Example: Improve customer experience, resulting in new income



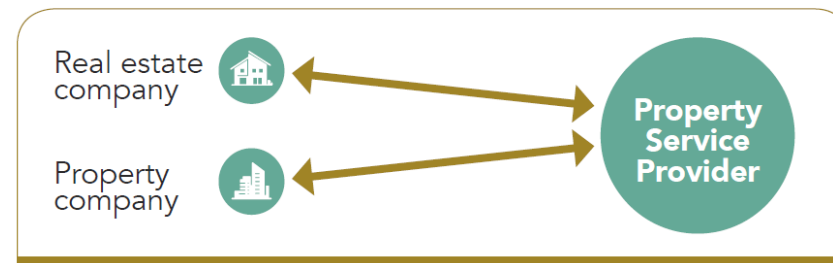
**b** Example: Improve overall efficiency over supply chain, resulting in cost reduction



**c** Example: Provide comprehensive information for overall market efficiency for the sector



**d** Example: Provide comprehensive information for public good



Provide a neutral and open **platform** for stakeholders to collaborate and promote big data development

Promote good **self-governance** for the big data industry

Establish big data governance **principles** and publish best practices

Guide and provide **oversight** on members' adherence to governance principles

**Facilitate** innovation and big data technological development

Act as conduit among international governments on **cross border** data sharing

## Advisory Board

- **Mr. Stephen WONG** (former Privacy Commissioner for Personal Data)
- **Mr. DU Ping 杜平** (Secretary-General of the National 13th Five-Year Plan Expert Committee, former Deputy Director of the State Information Center)
- **Prof. TSUI Lap Chee**, GBM, OC, O.Ont, JP (Founding President of the Academy of Sciences of Hong Kong)
- **Mr. Johnny MOK Shiu-luen**, SC, BBS, JP (Hong Kong Basic Law Committee member)
- **Dr. Lee George LAM**, (Chairman of Hong Kong Cyberport Management Co., Ltd.)

## Chairman

- **Ir. Allen YEUNG**, Former Hong Kong Government CIO

## Vice Chairman

- **Mr. Vincent CHAN**, Partner (Advisory Services), EY
- **Mr. Rocky CHENG**, GM, BOC (HK)
- **Mr. Herbert CHIA**, Venture Partner of Sequoia Capital China

## Founding Council Members

- **Ms. Cally CHAN**, GM (Hong Kong and Macau), Microsoft
- **Mr. Yam Ki CHAN**, Cloud Public Policy (Asia Pacific), Google
- **Ms. Selina LAU**, CE, HK Federation of Insurers
- **Mr. Alick LIU**, Chief Strategist, Greater China, SAP
- **Mr. Leo LIU**, GM (HKT Region), Alibaba Cloud
- **Mr. Gary YEUNG**, President of Smart City Consortium
- **Mr. Norman TAM**, GM, International Business, Tencent
- **Mr. Albert WONG**, CEO, HKSTP
- **Dr. CP WONG**, Chairman, HK Society of Medical Informatics

## Secretary General

**Dr. Charleston SIN**

## Asst. Secretary General

**Mr. Edwin LO**

## Treasurer

**Mr. Argon HO**

# iBDG

## Inauguration on Dec 5, 2018

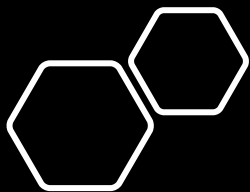




Data Governance  
Principles on par with  
global Best Practices



World's leading  
Data Governance  
Certification Scheme



# iBDG Big Data Governance Principles

## 大數據治理原則

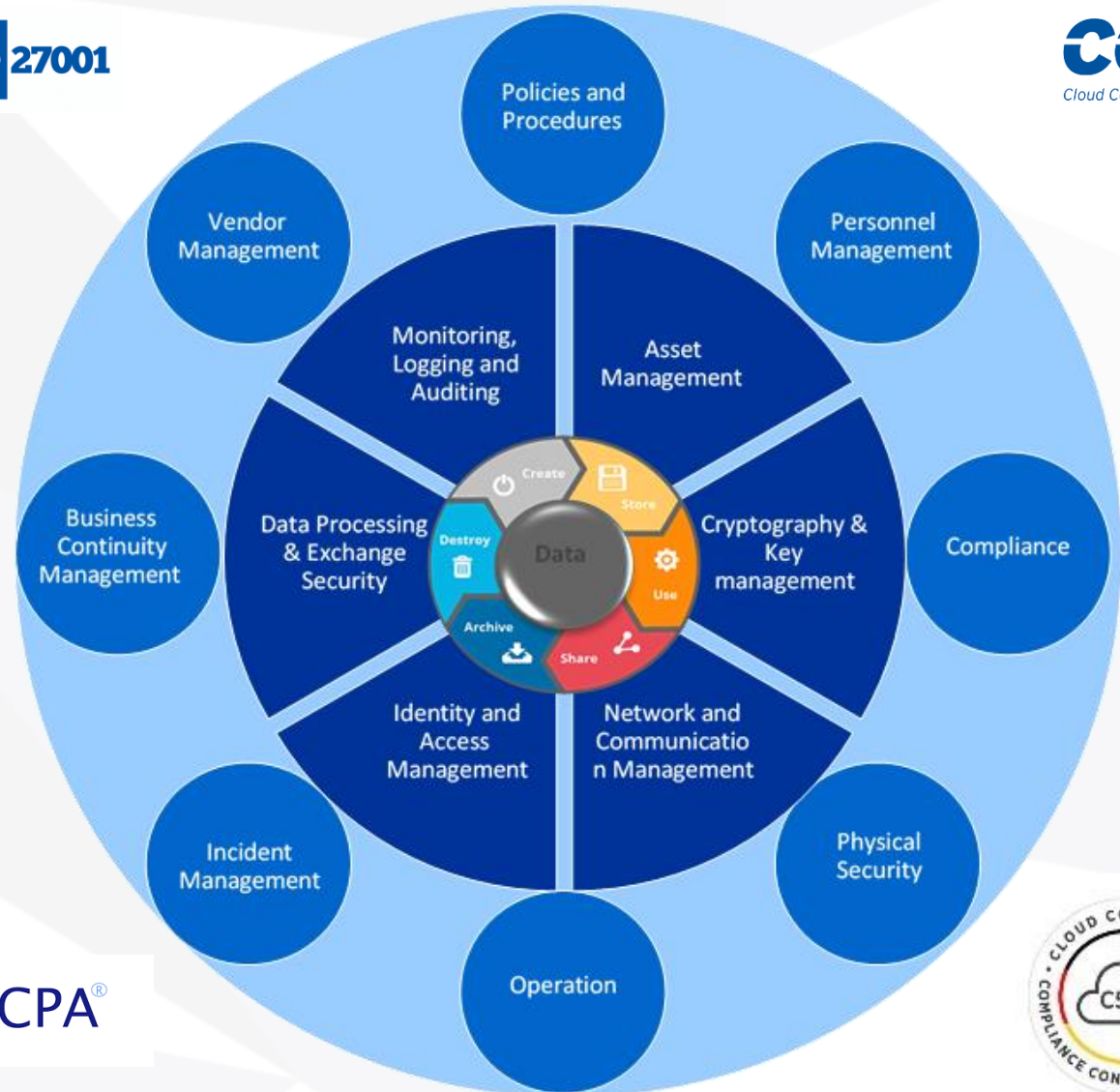
## iBDG Principles

- **P1. Data Processing**  
數據處理
- **P2. Personal Data Breach**  
數據外洩
- **P3. Data Transfer (or Sharing)**  
數據轉移
- **P4. Data Retention and Security Control**  
數據保留和安全控制原則
- **P5. Continuous Improvement**  
持續改進



# iBDG Big Data Governance Independent Assessment Scheme

- ◆ Information Security Technology- Guidelines for Data Cross-Border Transfer Security Assessment (信息安全技术-数据出境安全指南)
- ◆ Information security techniques — Data Security Capability Maturity Model (信息安全技术-数据安全能力成熟度模型)
- ◆ Information Security Technology- Baseline for Cybersecurity Classified Protection (Part1 : Security General Requirements) - Level 3 (信息安全技术-信息系统安全等级保护测评要求 – 通用三级)
- ◆ ISO/IEC 270001:2013
- ◆ CSA-Cloud Controls Matrix 3.0.1
- ◆ BSI- Cloud Computing Compliance Controls Catalogue
- ◆ AICPA - Trust Services Principles Criteria 2017
- ◆ Cloud Computing Compliance Controls Catalogue (C5)





iBDG 大数据治理评估标准				国内数据安全标准				国际数据安全标准			
	控制领域		控制分类	信息安全技术-数据安全能力成熟度模型	信息安全技术-数据出境安全指南	信息安全技术-信息系统安全等级保护测评要求-通用三级	个人信息出境安全评估办法(征求意见稿)	ISO/IEC 270001:2013	BSI-云计算合规控制目录	CSA-云控制矩阵 3.0.1	AICPA-信任服务原则标准 2017
				Ref.	Ref.	Ref.	Ref.	Ref.	Ref.	Ref.	Ref.
A	资产管理	A1	资产清单, 职责, 操作指南	PA23	5.2.5.2.a.2 5.2.5.2.a.3	7.2.3.1 7.2.3.2 7.2.4.2	-	A.8.1.1 A.8.1.2 A.8.1.3	AM-01 AM-02 AM-03	DCS-01 DSI-02 DSI-06 GRM-02 MOS-09	CC6.1
		A2	资产分类	PA01 PA23 PA25	5.2.5.2.a.2	7.2.3.1 7.2.3.2 7.2.4.2	-	A.8.2.1	AM-05	DSI-01	CC2.1 CC3.2 CC6.1 PI1.1 C1.1
		A3	资产的标记和处理	PA12 PA23	5.2.5.2.a.2 5.2.5.3.b	7.2.4.2	-	A.8.1.4 A.8.2.2 A.8.2.3	AM-04 AM-06	DSI-04	CC6.1 C1.1 PI1.1 PI1.5
		A4	数据媒体的管理	PA07	5.2.5.3.f	7.2.4.3	-	A.8.3.1 A.8.3.3	AM-07	DSI-05	CC6.5 CC6.7
		A5	资产处置	PA18 PA19	5.2.5.2.a.2	7.1.4.9 7.2.4.4.d	Clause 15	A.8.3.2 A.11.2.5 A.11.2.7	AM-04 AM-07 AM-08	DCS-04 DCS-05 DSI-07	CC6.5 CC6.7 C1.2 P4.3

# iBDG Data Governance Certification Independent Vetting Committee

## Chairman

- **Mr. Stephen WONG**  
former Privacy Commissioner for Personal Data

## Members

- **Mr Simon Chan**  
Chairman, Hong Kong Internet Registration Corporation Limited;  
Executive  
Director and Chief Executive, Nanyang Commercial Bank Limited
- **Mr Raymond Cheng**  
former Chief Operating Officer, HSBC
- **Mr Hugh Chow**  
CEO, Hong Kong Applied Science and Technology Research Institute  
(ASTRI)
- **Dr Lee George Lam**  
Chairman, Hong Kong Cyberport Management Company Limited
- **Johnny Mok SC, BBS, JP**  
Hong Kong Basic Law Expert

## Role and function of the Vetting Committee

The primary role of the Committee is to act as the decision-making body for iBDG on matters of both data governance certification application vetting and assessment scheme auditor approval, in particular with four principal functions:

1. to provide advices to the Council of iBDG on the certification vetting process;
2. to approve or disapprove certification applicants based on the audit reports from independent third-party auditors;
3. to remove an organization from the iBDG's Register of Certified Members in the event where the concerning organization no longer meets the requirements of a Certified Member; and
4. to review the iBDG's Register of Certified Members, at least annually, to ensure accuracy of their certified status.

- The Hong Kong Monetary Authority is introducing the Commercial Data Interchange (CDI), which aims to establish a consent-based common standard for data owners to share their digital footprint with banks through data providers
- IBDG advocates companies must be certified by IBDG to qualify for CDI in order to assure data quality and protection



- Set Data Strategy as a company-wide and unified strategy
  - Define how data can create values for business
- Develop Data Governance Framework, including
  - Define roles and responsibilities and Data Governance Personnel
  - Conduct data inventory check and determine third-party data requirements
  - Define data collection rules and regulations
  - Define Data sharing rules and regulations between business units and with outside parties
  - Establish solid data protection, privacy compliance and cybersecurity protection
    - Need to balance the business needs vs privacy protection vs cybersecurity
- Get IBDG certification to build trust for your clients
  - Position privacy protection as competitive advantage

An illustration of several hands of different skin tones and sleeve colors (yellow, brown, red, purple, blue, green) reaching towards the center of the frame. The background is a light green gradient.

# Collaborations

THANK YOU

---