Institute of Big Data Governance (iBDG)
Big Data Governance Principles 3.1

A. Objectives

1. iBDG sets out the Big Data Governance Principles ('Principles') in order to build Hong Kong as an international data hub; raise the data governance of Hong Kong enterprises to world standards; support Hong Kong enterprises making use of big data to conduct digital business; and build up trust for facilitating cross-border data transfers between Hong Kong, the mainland of China, and the rest of the world.

2. iBDG believes technology will continue to shape the big data governance landscape in the future and will refine the Principles accordingly.

B. Scope

1. The Principles apply to pledged and certified members of iBDG that are Hong Kong-based data controllers ('HKDC') handling big data ('data'), including personal data and government regulated data, with reference to international standards, applicable laws and regulations.

2. Defined terms are set in Appendix A of this document.

C. Principles

1. Big data accountability principle

a. The HKDC must set up data governance organisation structure and plan to be responsible for compliance, accountability, data quality management and data protection, including the following measures:

   i. establish an organization structure that matches with company culture, with the data governance role of senior management defined clearly;
   ii. establish big data exchange standards to provide safe, efficient and reliable data exchange for data transfer;
   iii. define job roles and responsibilities for big data governance;
   iv. define big data governance related processes and procedures that enable control and

management of big data processing activities;

v. compile policies, administrative measures and operating rules as needed to provide standard instructions for execution;
vi. put data security as a core element to protect data, establish internal review and approval processes and keep relevant information for examination and audit purpose;
vii. provide education and training sessions to raise staff members' awareness of the importance of data management

2. Big data processing principle

a. Data is collected only for specified, explicit and legitimate purposes; and not further processed in any manner that is not primarily intended to achieve those purposes, unless anonymized.
b. Data must be processed lawfully based on the principles of fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, meaning:
   i. data is processed based on the specified, explicit and legitimate purposes during data collection processes;
   ii. only relevant and necessary data in relation to the purposes should be processed, and should be limited to the minimum scope for realization of the data processing purpose without excessive collection of information;
   iii. best efforts are made to ensure that data processed is accurate, and, where necessary, complete and up-to-date, strengthen technical management;
   iv. data processing activities are controlled in a secured and confidential manner in accordance with regulatory, compliance and information security requirements, regular review and evaluation, improve the working mechanism of data processing;
   v. any data applications leading to discrimination and/or re-identification of customers should be avoided;
   vi. use tools or automatic procedures as needed to support big data processing;
   vii. Ethical Data Impact Assessments (EDIAs)[1] must be conducted when advanced-data analytics may impact concerned persons in a significant manner and/or when data-enabled decisions are being made without the intervention of people. Impact assessments for both risks and benefits to the organization, the customers and the society (if applicable) must be conducted.

c. The requirements of customer consent for personal data processing are:

[1] EDIA – a means of determining whether an instance of processing is in accordance with the data stewardship values and guiding principles established by the organization.

i. default setting for ‘consent’ is not allowed and such consent should be obtained in an intelligible and easily accessible form using clear and plain language;
ii. customers should be clearly informed of their rights, and the method by which, to withdraw their consents given;
iii. customers have the rights to request for access of their own personal data from data controller and to obtain the confirmation from the data controller whether the personal data concerning him or her are being processed or not, and for rectification of inaccurate personal data concerning them without undue delay;
iv. no bundling of the customer consent for different applications should be made;
v. HKDC should not refuse to provide products or services if a customer does not provide or withdraw the consent with personal information provided except where personal information is needed for products or services provision;
vi. Where two or more HKDCs jointly decide the purpose and method of the personal information handling, they should agree on the rights and obligations of each other and inform the customers affected;
vii. Where HKDC entrusts the processing of customers’ personal data, it should conclude an agreement with the entrusted party on the purpose of data processing, the method of data processing (including if engagement of other parties is allowed), duration, the categories and scope of personal information, the protection measures, as well as the right and obligation of both parties. HKDC should supervise the personal data processing activities of the entrusted party. Entrusted party should handle personal data in accordance with the contract or agreement, and should not handle personal data beyond the agreed processing purpose, methods and timeline, and should delete or return the personal data after the contract is completed or when the entrusted relationship is terminated;
viii. If the entrusted party requires to engage another party to carry out the entrusted data processing activities, it should inform HKDC, and obtain approval as well as authorization from HKDC prior to the beginning of such activities, or such activities should not be allowed. HKDC reserves the right to request the entrusted party to provide relevant data processing agreement and/or contract, and information about how the entrusted party monitor the activities.
ix. When using personal information to conduct automated decision making, HKDC should be able to explain on what personal data that the decision made is based upon and demonstrate explainability of the decision-making model, and ensure the fairness and reasonability of the processing result. Where customers consider automated decision making having impact to their rights and interests, they should have the rights to request for explanations from HKDC.
x. By the time personal data are obtained, organizations shall provide the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.

d. Organizations must keep audit logs for all the data processing activities such as the date, time, types of data processed and the purpose of processing. Data processing methodologies and rules must be documented and abided.

e. Conduct data classification to improve data visualization and ensure security of data processing and transmission:
   (1). Identify classification objects: such as data items, data sets, derived data, cross-industry domain data, etc;
   (2). Determine classification elements: domains, groups, regions, precision, scales, depth, coverage, importance, etc;
   (3). Determine degree of impact: national security, economic operation, social order, public interests, organizational rights and interests, and individual rights and interests.

f. Review and approval process must be established for any special data processing activities, where sufficient information must be provided as supporting evidence for such exceptions made such as those involving substantial public interest or in the course of its legitimate activities with appropriate safeguards (e.g. statutory purposes, regulatory requirements, and preventing or detecting unlawful acts etc.)

g. Organizations must make clear to customers, prior to services provision, that the relevant services are powered by big data analytics and artificial intelligence (BDAI) technology and state the associated risks, if any. For use of personal data for development of BDAI applications, categories and scope of personal data used must be documented to ensure that personal data used are relevant, accurate and complete, and appropriate data security measures are imposed.

h. If a consent for collection and use of personal data in relation to a product or service powered by BDAI technology is required, it should be as clear and understandable as possible in the interests of ensuring informed consent. Periodic review and continuous optimization mechanism on BDAI should be conducted to protect personal data security and customer rights.

i. When organizations use generative AI technology to process data, they need to identify generated content such as text, pictures, audio and video:
   (1). Explicit watermark identification with translucent text added within an interface or in the background
   (2). Implicit watermark identification with an identifier added by modifying the content of a picture, audio, or video that is not directly accessible to humans but can be extracted from the content by technical means.

j. Identification method and identification information of generative AI:
   (1). Make corresponding prompts in the explicit area of the AI -generated content, including but not limited to the bottom of the explicit area, the bottom of the user input information area, and the background of the explicit area, where prompt texts should contain information such as artificial intelligence generation;
   (2). When images, audio, and video are generated by artificial intelligence, implicit watermark identification should be added to the generated content, and the identification content should contain at least the service provider and content ID;
   (3). The extension field should be added to the metadata file for identification, and the extension field should contain the service provider name, content generation time, content ID and other information.

k. If the organization needs to transfer personal information due to merger, division, dissolution, declaration of bankruptcy, etc., it shall inform the customer of the data recipient's name or name and contact information. Data recipients shall continue to perform its obligations as a personal information processor. If the data recipient changes the original processing purpose and processing method, it shall obtain personal consent again in accordance with this principle.

l. If the data processor uses biometrics for personal identity authentication, it shall conduct a risk assessment on necessity and security, and shall not use biometrics such as face, gait, fingerprint, iris, voiceprint and other biometrics as the only personal identity authentication method to force individuals to consent to the collection of their personal biometric information.

m. Further processing of data for public interest, scientific or historical research purposes or statistical purposes shall be subject to appropriate safeguards, to protect the rights and freedoms of data subjects.

3. Data retention and security control principle

a. Organizations must develop a data retention policy, which specifies the retention period (including for the shortest and the longest retention period) according to applicable laws and regulations, and supported with storage management procedures and other documentation obligations. Apart from fulfilling the regulatory requirements, data must be prevented from being kept for a period longer than as needed.

b. Customers have the rights to request for deletion of their personal data retained in the organizations without undue delay in the following circumstances.

   i. the consent to provide the personal data for processing is withdrawn by customers;

ii. the personal data provided for the original purposes is no longer applicable;
iii. there is no overriding legitimate interest.

c. Organizations should formulate internal management systems and operating procedures, implement security classification management of data, and select corresponding security measures according to different data classification. Regular tests and evaluations should be made for security of data processing and control measures taken by the organization.

d. Data should be protected with consideration of its sensitivity during data aggregation and data classification, such as data isolation or other mechanisms to ensure sensitive information will not be exposed when large amount of data is aggregated, and sensitive data should be classified with access controls made.

e. Organizations must develop an information security strategy, where data needs to be secured in the entire data life cycle including the three states of data at rest, data in use and data in motion.

f. Data encryption features, anonymization, de-identification, access control security measures and strong password protection measures, whichever appropriate, must be in place for data storage, data processing and data transfer especially with personal data.

g. Organizations using generative AI for models pre-training and data processing have to follow corpus security and models security guidelines, and to ensure security measures and assessments made regularly:
   (1). Corpus security requirements
      A. Security of the corpus's sources should be assessed;
      B. Organize safety trainings, use of keywords, classification models and manual inspection to filter illegal information in the corpus.
   (2). Model security requirements
      A. If services need to be provided based on a third-party's model, the organization should use the base models adopted by concerned departments and regulatory authorities;
      B. Technical measures should be taken to improve data consistency and expressions in the generated contents to enhance matching with scientific knowledge and mainstream cognition in order to reduce wrong contents;
      C. Technical measures should be taken to improve reasonablness of the generated contents' format and the degree of effective contents so as to add more values to users.
   (3). Security measure requirements
      A. Fully demonstrate needs, applicability and security to apply generative artificial intelligence in various fields of the model within the scope of service;

B. Provide channels and feedback methods for receiving complaints and reports from the public or users, including but not limited to one or more means such as telephone, mail, interactive Windows, SMS, etc;
C. Develop security management policies for model updates and upgrades;
D. Isolate the training environment from the inference environment to avoid data leakage and improper access.

(4). Security assessment requirements

A. Security assessment report should include the conclusion of the overall assessment after evaluating corpus security and contents of generated by models, the details of which can be referred to《生成式人工智能服务安全基本要求》.

h. HKDC shall establish a data security emergency response mechanism, data transmission and data processing shall be terminated immediately, activate an emergency response mechanism in a timely manner when a data security incident occurs, and take measures to prevent the expansion of hazards and eliminate potential security risks, protect the rights and interests of data subjects.

i. When a data security incident occurs, the relevant information should be reported to the local regulatory authorities, including the threat to the rights and interests of data subjects, causes, and emergency measures.

4. Personal data breach prevention principle

a. In the case of a personal data breach, which is likely to result in a risk to the rights and freedoms of the customer, the HKDC should notify the relevant supervisory authority, without undue delay and, where feasible, not later than 72 hours after having become aware of it. Where the notification to the relevant supervisory authority is not made within 72 hours, it should be accompanied by reasons for the delay.

b. The HKDC must ensure that the data processor will notify the HKDC without undue delay after becoming aware of a personal data breach.

c. HKDC must conduct a risk assessment without undue delay after becoming aware of a personal data breach. The assessment shall contain at least:

i. an assessment of categories, content, security level and volume of personal data concerned, as well as the approximate number of customers concerned;
ii. an assessment of the possibility to identify the customer from the personal data concerned;
iii. an assessment of potential consequences or negative impacts brought by the personal data concerned;

d. The notification referred to in C.4.a must at least:
   i. describe the reason, the nature of the personal data breach and the assessment specified in C.4.c;
   ii. communicate the name and contact details of contact point where more information can be obtained;
   iii. describe the likely consequences of the personal data breach;
   iv. describe the measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

e. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

f. The HKDC must document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. Such documents should enable regulatory bodies evaluate whether the big data governance principles are adhered.

g. Where the personal data breach is likely to result in a high risk to the rights and freedoms of the customer(s) (such as discrimination, identity theft, fraud, financial loss, or damage to their reputation), the HKDC shall communicate the personal data breach to the customer(s) without undue delay. The communication to the customers shall describe in clear and plain language the nature of the personal data breach containing at least the information and the recommendations provided in C.4.d. ii, iii and iv above.

h. The communication to the customer(s) referred to in C.4.g above shall not be required if any of the following conditions are met:
   i. The HKDC has implemented appropriate technical and organizational protection measures, and that those measures where applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;
   ii. The HKDC has taken subsequent measures which ensure that the high risk to the rights and freedoms of customers referred to in C.3.f above is no longer likely to materialize;
   iii. It would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the customers are informed in an equally effective matter.

i. Organizations should take the following measures to prevent unauthorized access and leakage, tampering, and loss of personal information according to the purpose of processing personal

information, processing methods, types of personal information, impact on personal rights and interests, and possible security risks:

i. Formulate internal management systems and operating procedures;
ii. Reasonably determine the operation authority of personal information processing, review the operation authority regularly regularly and conduct security education and training for employees on a regular basis;
iii. Formulate and organize the implementation of contingency plans for personal information security incidents.

j. Departments performing personal information protection duties perform the following personal information protection duties:
   i. Carry out publicity and education on personal information protection, and guide and supervise personal information processors to carry out personal information protection work;
   ii. Assess application procedures regularly in terms of personal information protection, and publish the assessment results for record;
   iii. Investigate and handle illegal personal information processing activities, and cooperate with the investigation from regulators or law-enforcement agencies when necessary.

5. Data transfer principle

a. Data transfer within Hong Kong and cross border boundary is encouraged to facilitate digital business, as long as the following conditions are met:
   i. HKDC must ensure, through contractual or other means, that data continues to be protected to a comparable standard as if it had remained with the HKDC. In other words, HKDC must continue to be accountable for the data even after data transfer has happened.
   ii. the HKDC receiving the data must be a certified member of iBDG that has implemented adequate data protection capabilities to protect the data.

b. Data re-transfer beyond the scope of application is not allowed unless customer consent has been sought. The scope of application is referred to collection and use of data stated in the notice to customers and the data policy, if any.

c. The following measures must be taken for data transfer:
   i. organizations must implement effective controls to prohibit unauthorized data transfer;
   ii. organizations must implement necessary security measures to prohibit unauthorized access of data or data leakage during data transfer;
   iii. data transfer is only allowed through legitimate channels and in a secured format;

iv. data transfer activity records including the data recipient, region/country, the purpose, type and volume of data processed etc. must be clearly documented.

d. Prerequisite of cross border data transfer is as follows:
   i. the data for transfer is not the type defined and prohibited by local regulations.
   ii. data exporters and data recipients must formulate and sign a cross-border data transfer agreement or contract with reference to relevant and applicable standard or model contractual clauses[2], or conduct necessary security assessment on the cross-border data transfer activities, including the use of data by the data recipients in accordance with the purpose, scope and approaches agreed by both parties.
   iii. data exporters must ensure that the data will be still protected in terms of safety and confidentiality after transfer by means of regulations or legal agreements reached with data recipients.
   iv. data exporters' fundamental rights of using the data will not be changed after transfer.
   v. Both parties have taken appropriate steps to determine the level of potential risk of data breaches involved in transferring the relevant data and to consider suitable security that both parties must undertake.
   vi. Both parties shall agree on and implement appropriate controls and adequate security standards that shall apply to the storage and Processing of Personal Data.

e. Cross border data transfer security assessment must be made based on:
   i. the legality, legitimacy and necessity of the purpose, scope and mode of data transmission;
   ii. the agreement, if any, from the customers or individuals;
   iii. the quantity, the scope, the types and the sensitivity of personal data concerned, list of data fields and identification of the path for cross-border data transfer;
   iv. the obligations undertaken by data recipients, as well as the security measures, functions, security levels and local cybersecurity environment adopted to secure protection of personal information during cross-border transfer;
   v. risk of data being re-transmitted, amended, destroyed, leaked, lost, transferred or illegally obtained or used after transmission;
   vi. the risks to national security, public interest, and personal legal interests posed by the data transferred;
   vii. the security assessment should be conducted by an independent third party;
   viii. the customers' or individuals' personal interest may be infringed, or there exists risks posed

[2] For example: Guidance on Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data, Office of the Privacy Commissioner for Personal Data, Hong Kong; Measures on the Standard Contract for Cross-border Transfers of Personal Information, Cyberspace Administration of China; Standard Contractual Clauses for Data Transfers between EU and Non-EU Countries, European Commission; Model Contractual Clauses for Cross Border Data Flows, Association of Southeast Asian Nations; etc.

to the countries concerned due to the data transfer

f. Anonymized data can be transferred based on business agreement. HKDC of the data recipient must not use or attempt to use anonymized data to re-identify any individual.

g. For the data processed by artificial intelligence, an explicit watermark should be made if missing before continuation of data transmission.

h. Cross border/boundary enterprises business data transferred to the HKDC from a non-Hong Kong-based data controller should be processed in compliance with the laws and regulations of the region or country of the non-Hong Kong-based data controller. Such enterprise business data should not be further transferred to other regions or countries without consent from the original data controller.

i. Assign data security stewards as required to coordinate data security supervision and management for data processing activities.

j. For cross-border transfer of personal information, HKDC should inform customers about the data recipient, the purpose and methods of data processing, and their rights etc., and obtain separate consents from customers.

k. HKDC should conduct regular audit and inspection on the data recipients' operations including any contractors, service providers and the third parties to ascertain their compliance with their obligations under the data transfer agreement.

l. HKDC should adopt contractual or other means to prevent the personal data from being retained by the data recipient after fulfillment of the purpose(s) for which the personal data is disclosed or transferred.

m. HKDC should pass the customer rectification and/or deletion request to the data recipient, who should rectify, erase or return the personal data on receiving instruction to the request without undue delay.

6. Data sharing principle

a. Data sharing within the organization that complies with data security requirements is encouraged to promote data applications and digital business;

b. Data sharing between organizations is encouraged to facilitate digital business, as long as the following conditions are met:

i. HKDC must ensure, through contractual or other means, that data continues to be protected to a comparable standard as if it had remained with the HKDC. In other words, HKDC must continue to be accountable for the data even after data transfer has happened.

ii. the HKDC receiving the data must be a certified member of iBDG that has implemented adequate data protection capabilities to protect the data.

c. Anonymous data may be shared in accordance with the agreement, but the HKDC of the data recipient shall not use the anonymized data to re-identify any individuals.

7. Continuous improvement principle

a. Pledged and certified members must continuously improve their data governance practices by adopting data management principles with reference to international standards and global industry best practices.

b. Pledged and certified members of the iBDG must conduct annual data audit by an independent third-party auditor accredited by iBDG.

c. Pledged and certified members are recommended to appoint designated positions (e.g. Data Protection Officer (DPO)) to formulate and review policies and procedures to prevent the areas that may lead to potential risks such as data leakage and personal data breaching. When risks such as data security defects and loopholes are discovered, remedial measures shall be taken immediately; when data security incidents occur, disposition measures shall be taken immediately, users shall be notified in a timely manner and reported to relevant competent authorities in accordance with regulations.

d. Pledged and certified members must assess the ever-changing regulatory, economic and/or technological changes brought to their compliance level.

e. Data mining, analytics, artificial intelligence and profiling techniques may, either inadvertently or purposefully, expose one's innermost secrets, or intimate space. HKDC must constantly review if the data protection measures taken are sufficient to protect both organizational and public interests, strengthen responsibilities and conduct regular reviews on data processing and data transmission in the whole data life cycle.

f. Members can seek support from iBDG for unclear scenario or undefined use cases.

Information Reference Sources:

1. General Data Protection Regulation (GDPR) (https://gdpr-info.eu/)
2. Hong Kong Monetary Authority: Customer Data Protection (https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2014/20141014e1.pdf)
3. Privacy Commissioner for Personal Data: The Personal Data (Privacy) Ordinance (the 'PDPO') (https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html)
4. APEC Privacy Framework (https://apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015))
5. Personal Information Protection Law of the People's Republic of China (http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml)
6. Privacy Commissioner for Personal Data: Guidance on Personal Data Protection in Cross-border Data Transfer (https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_crossborder_e.pdf)
7. Hong Kong Monetary Authority: Consumer Protection in respect of Use of Big Data Analytics and Artificial Intelligence by Authorized Institutions (Nov 2019) (https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191105e1.pdf)
8. 《金融数据安全 数据安全分级指南》(https://www.cfstc.org/bzgk/gk/view/yulan.jsp?i_id=1873)
9. 《信息安全技术 大数据安全管理指南》(http://c.gb688.cn/bzgk/gb/showGb?type=online&hcno=D16FF5DF1E14AF4D3263C0D8FED78579)
10. 《中国银保监会监管数据安全管理办法（试行）》(http://www.cbirc.gov.cn/cn/view/pages/govermentDetail.html?docId=959801&itemId=861&generaltype=1)
11. Data Security Law of the People's Republic of China (http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml)
12. 《网络数据安全管理条例（征求意见稿）》(http://www.cac.gov.cn/2021-11/14/c_1638501991577898.htm)
13. ASEAN Model Contractual Clauses for Cross Border Data Flows (https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf)
14. Hong Kong Monetary Authority: Circular on High-level Principles on Artificial Intelligence (https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191101e1.pdf)
15. European Data Protection Board: Guidelines 9/2022 on personal data breach notification under GDPR (https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf)
16. Cyberspace Administration of China: Measures on the Standard Contract for Cross-border Transfers of Personal Information

17. European Commission: Standard Contractual Clauses for Data Transfers between EU and Non-EU Countries
18. 《建设全国一体化政务大数据体系 推进国家治理体系和治理能力现代化》(https://www.gov.cn/zhengce/2022-11/01/content_5723178.htm)
19. 《互联网信息服务深度合成管理规定》(https://www.pcpd.org.hk/misc/dopc/newsletter153.html#mainland)
20. Data security technical data classification and classification rules (https://www.tc260.org.cn/upload/2024-03-21/1711023239820042113.pdf)
21. 《网络安全标准实践指南 – 生成式人工智能服务内容标识方法》(https://www.tc260.org.cn/upload/2023-08-25/1692961404507050376.pdf)
22. Personal Information Protection Law (https://www.pcpd.org.hk/tc_chi/data_privacy_law/mainland_law/mainland_law.html)
23. Basic requirements for security of generative AI services (https://www.tc260.org.cn/upload/2024-03-01/1709282398070082466.pdf)
24. 《信息安全技术 数据出境安全评估指南》(https://www.tc260.org.cn/ueditor/jsp/upload/20170527/87491495878030102.pdf)
25. Network data security management regulations (https://www.cac.gov.cn/2021-11/14/c_1638501991577898.htm)
26. 《数据出境安全评估办法》(https://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm)
27. 《网络数据安全管理条例（征求意见稿）》 (https://www.cac.gov.cn/2021-11/14/c_1638501991577898.htm)
28. Greater Bay Area Standard Contract (https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/standard_contract_gba.pdf)
29. 《互联网信息服务算法推荐管理规定》 (https://www.cac.gov.cn/2022-01/04/c_1642894606364259.htm)
30. 《工业和信息化领域数据安全管理办法（试行）的通知》(https://www.gov.cn/zhengce/zhengceku/2022-12/14/content_5731918.htm)
31. 《生成式人工智能服务管理暂行办法》(https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm)
32. 《互联网信息服务深度合成管理规定》(https://www.cac.gov.cn/2022-12/11/c_1672221949318230.htm)
33. 《新一代人工智能伦理规范》(https://www.most.gov.cn/kjbgz/202109/t20210926_177063.html)

Appendix A – Glossary

For the purposes of the Principles:

1. The customer's "consent" refers to any specific, informed and clear instructions freely given by the customer. personal data wishes.

2. “Cross-border/cross-border data" refers to data transferred from other jurisdictions to Hong Kong, China.

3. "Data source region or country" refers to the jurisdiction where the data is generated.

4. ‘*certified member’* is a member of the iBDG that has been deemed certified against the iBDG certification scheme by an independent third-party auditor accredited by iBDG.

5. ‘pledged member’ is a member of the iBDG that has pledged to the big data governance principles.

6. ‘data controller’
   a. if the purposes and means of processing data are determined by iBDG or Hong Kong law, the data controller means the controller or the specific criteria for its nomination may be provided for by iBDG or Hong Kong law.
   b. if the purposes and means of processing data are not determined by iBDG or Hong Kong law, the data controller means agency or enterprise which, alone or jointly with others, determines the purposes and means of the processing of data.

7. ‘data minimization’ means personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

8. ‘enterprise’ means a legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity.

9. ‘enterprise business data’ is business related data that is shared by the users of an enterprise, generally across departments and/or geographic regions. Enterprise business data include data that originates from the HKDC, data transferred from other Hong Kong-based data controller(s) to the HKDC, or data transferred from non-Hong Kong-based data controller(s) to the HKDC.

10. ‘government regulated data’ is data used by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal

penalties, including the safeguarding against and the prevention of threats to public security.

11. ‘Hong Kong-based data controller’ or ‘HKDC’ is a data controller incorporated in Hong Kong.

12. ‘non-Hong Kong-based data controller’ is a data controller that is not incorporated in Hong Kong.

13. ‘personal data’ means any information relating to an identified or identifiable natural person.

14. "Third parties" means natural or legal persons, public authorities, departments or bodies autherized by customers, controllers, processors and persons authorized to process personal data.

15. ‘identified or identifiable natural person’ is a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, mac ID, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

16. ‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

17. ‘processing’ means any operation or set of operations which is performed on data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

18. ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

19. ‘representative’ means a natural person or a legal person established in Hong Kong, China, who performs its obligations under these Principles on behalf of the controller or processor.

20. ‘regulator’ means an independent public body established or recognized by iBDG.