Alibaba Cloud User Guide
on
Hong Kong Personal Data (Privacy) Ordinance (Cap. 486)

May 2019

Alibaba Cloud | Worldwide Cloud Services Partner

Notices

Background

The data protection law in Hong Kong is the Personal Data (Privacy) Ordinance (Cap. 486). It came into force in 1996, a year after the European Data Protection Directive 95/46/EC, and it shares many of the base principles from the directive. The main objective is to protect the privacy rights of a person in relation to personal data (data subject). The Amendment Bill, relating to the regulation of the use of personal data for direct marketing purposes, was passed by the Legislative Council June 27, 2012.

According to the ordinance, a data user is defined as “a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data.” In this case, the data user is equivalent to the controller role in GDPR, while the third party is similar to the processor role in the GDPR, and a data processor is defined under the 2012 amendment. The data user, not the third party or data processor, is liable as the principal for the wrongful act of its authorized data processor. This is similar to the Directive 95/46/EC, whereas the GDPR holds both the controller and processor liable. (*See the comparison table at the end of the document for additional reference details.)*

The ordinance includes six data protection principles, and “everyone who is responsible for handling data (Data User) should follow the six Data Protection Principles ("DPPs") which represents the core of the Ordinance covering the life cycle of a piece of personal data.”

DPP1 — Data Collection Principle

The first principle states that “personal data must be collected in a lawful and fair way, for a purpose directly related to a function/activity of the data user. Data subjects must be notified of the purpose and the classes of persons to whom the data may be transferred.”

Alibaba Cloud is committed to protect customer personal information and guarantees that such information is only used for the purposes agreed to by customers. Alibaba Cloud's privacy policy describes how we collect personal information, as well as the purposes for the collection, retention, use, disclosure and transfer of personal data.

DPP2 — Accuracy & Retention Principle

Under the ordinance, “practicable steps shall be taken to ensure personal data is accurate and not kept longer than is necessary to fulfill the purpose for which it is used.” At Alibaba Cloud, we retain customer personal data as long as a customer has an account with us, as needed to provide services or products to customers, to resolve disputes, or as required or permitted by applicable laws, such as tax and accounting laws.

DPP3 — Data Use Principle

The principle states that "Personal data must be used for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent with a new purpose is obtained from the data subject." The ordinance also mentions the situation when a data subject is incapable of providing consent (such as minors, and physically or mentally incapable individuals), a relevant person in relation may give the prescribed consent when dealing with a new purpose. Alibaba Cloud uses customer personal data to communicate with customers about our products and services and provide customers with marketing information. Those types of consent can be managed at the customer portal, and may subsequently be withdrawn at any time without affecting the lawfulness of processing based on consent before its withdrawal.

DPP4 — Data Security Principle

One can almost never have privacy without security. The ordinance also states the data security principle that "a data user needs to take practicable steps to safeguard personal data from unauthorized or accidental access, processing, erasure, loss or use." Under the GDPR, it requires the implementation of appropriate technical and organizational measures to ensure an appropriate level of security, and those measures also address the areas of confidentiality, integrity and availability of the data. However, the GDPR also includes provisions for breach notification, which is not noted in the ordinance.

Alibaba Cloud has published the latest version of our Security White Paper describing our security methodology. The whitepaper covers each of the following aspects, such as security policies, organizational security, compliance, data security, access control, personnel security, physical security, infrastructure security, systems and software development and maintenance, disaster recovery and business continuity. The content of the paper provides useful guidance on how our security practice can support the requirements in various compliance requirements. In 2017, Alibaba Cloud became the first cloud provider to attest to the additional requirements of the German C5 Criteria: to demonstrate our commitment to a higher security standard. Furthermore, Alibaba Cloud has established breach notification policies and procedures, and has conducted numerous drills to ensure that the teams involved are aware of their roles and responsibilities.

DPP5 — Openness Principle

Per the ordinance, "a data user must take practicable steps to make personal data policies and practices known to the public regarding the types of personal data it holds and how the data is used." This is also addressed under GDPR under the transparency and modalities as part of the data subject's rights. At Alibaba Cloud, customers have the right to request access to their personal data held by us (or on our behalf) and to request correction or deletion of such personal data. Our privacy practices are completely transparent to the public, and our Privacy Policy can be found on our official website at: https://www.alibabacloud.com/help/faq-detail/42425.htm

DPP6 — Data Access & Correction Principle

Under the last principle, "a data subject must be given access to his/her personal data and allowed to make corrections if it is inaccurate." As part of the effort to expand customer control over the use of personal data, the GDPR introduces new data subject rights. One is the Right to be Forgotten (GDPR article 17). Alibaba Cloud provides an account deletion function, which achieves systematic account deletion.

The ordinance also provides exceptions of personal data in areas such as: held domestic or recreational purposes; access requirement for certain employment related, "likely to prejudice security, defense and international relations; crime prevention or detection; assessment or collection of any tax or duty; news activities; health; legal proceeding; due diligence exercise; archiving; handling life-threatening emergency situation," etcetera.

Conclusion

Privacy starts at the design stage, but protection of data subject rights and privacy requires the accomplishment of many individual parts. Privacy by Design promotes privacy and data protection from the beginning. All of our newly released Alibaba Cloud products have been through a security review and a privacy design assessment to ensure security and privacy considerations are embedded in the product. Besides our commitment in meeting the Hong Kong Personal Data (Privacy) Ordinance requirements, Alibaba Cloud also obtained the TRUSTe Enterprise Privacy Certification, and met the requirements of Singapore's Personal Data Protection Act (PDPA). Experience with global requirements laid a foundation for GDPR and any future privacy compliance.

At Alibaba Cloud, we are committed to our customers around the world. We understand the importance of international data protection standards and will help ensure security interests for countries globally are respected.

Reference

Here is a comparison of some of the common topics between the Ordinance and the GDPR for an informational referencing purpose:

Topic	The Ordinance	GDPR
Personal Data	Any data: (a) Relating directly or indirectly to a living individual; (b) From which it is practicable for the identity of the individual to be directly or indirectly	Any information: (a) Relating to an identified or identifiable natural person; (b) An identifiable natural person is one who can be identified, directly or indirectly, in

Topic	The Ordinance	GDPR
	ascertained; and (c) In a form in which access to or processing of the data is practicable * Examples of personal data protected by the ordinance include names, phone numbers, addresses, identity card numbers, photos, medical records and employment records.	particular by reference to an identifier such as a name, an identification number, location data, 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.
Data Subject	In relation to personal data means the individual who is the subject of the data.	Relating to an identified or identifiable natural person.
Controller	"Data User": In relation to personal data, means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data.	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or member state law, the controller or the specific criteria for its nomination may be provided for by Union or member state law.
Processor	Part of the 2012 amendment, a Data Processor: (a) Processes personal data on behalf of another person; and (b) Does not process the data for any of the person's own purposes. Third Party: in relation to personal data, means any person other than: (a) the data subject; (b) a relevant person in the case of the data subject; (c) the data user; or (d) a person authorized in writing by the data user to collect, hold, process or use the data (i) under the direct control of the data user; or (ii) on behalf of the data user.	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. However, GDPR does also have a definition for "third party": A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.
Sensitive Data	None	Article 9: Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
Transfer of Personal Data to third countries or	No requirements on transfer of personal data to cross-border.	Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organization shall take place

Topic	The Ordinance	GDPR
international organizations		only if the conditions laid down in Article 44 – 50 are complied with by the controller and processor to ensure that the level of protection of natural persons guaranteed by the GDPR. Transfers on the basis of an adequacy decision and methods such as BCR, Contract Clauses, etc. or in the case of EU-US transfer, the Privacy Shield.
Data Portability	A data subject must be given access to his/her personal data and allowed to make corrections if it is inaccurate.	Article 20: The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.
Penalty	Noncompliance with Data Protection Principles does not constitute a criminal offense directly. The commissioner may serve an Enforcement Notice to direct the data user to remedy the contravention and/or instigate the prosecution action. Contravention of an enforcement notice is an offense which could result in a maximum fine of HK$50,000 and imprisonment for two years. An individual who suffers damage, including injured feelings, by reason of a contravention of the ordinance in relation to his or her personal data may seek compensation from the data user concerned. The ordinance also criminalizes misuse or inappropriate use of personal data in direct marketing activities (Part VI); noncompliance with Data Access Request (section 19); unauthorized disclosure of personal data obtained without data user's consent (section 64), etcetera	**Under** Article 83: • Up to 10 000 000 EUR, or in the case of an undertaking, up to 2 percent of the total worldwide annual turnover of the preceding financial year, whichever is higher for infringements of obligations such as controllers and processors, the certification body, and the monitoring body. • Up to 20 000 000 EUR, or in the case of an undertaking, up to 4 percent of the total worldwide annual turnover of the preceding financial year, whichever is higher for infringements of obligations such as principles of processing, conditions for consent, data subject's rights, transfer beyond EU, etcetera • Under Article 84, each member state can lay down the rules on other penalties applicable to infringements of GDPR in particular for infringements which are not subject to Article 83, and can take all measures necessary to ensure that they are implemented.