Comparing the GDPR and Hong Kong: Overview

by Chiang Ling Li and Carrie Chan, Georgiou Partnership, with Practical Law Data Privacy & Cybersecurity

Practice note: overview | Law stated as of 01-Jan-2026 | Asia, Hong Kong - PRC

A quick reference Chart comparing some of the key requirements of the Hong Kong Personal Data (Privacy) Ordinance (Cap 486) (Ordinance) and the EU General Data Protection Regulation (GDPR). This Chart does not cover every topic addressed by these laws or provide detailed guidance on necessary steps to comply with the laws.

Applicability of the GDPR and National Law

GDPR and Hong Kong Ordinance Comparison Chart

This Chart provides a high-level comparison of some of the key requirements under the Hong Kong Personal Data (Privacy) Ordinance (Cap 486) (Ordinance) and the EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR).

The GDPR explicitly requires non-EU-based organizations that engage in certain EU-related activities to comply with its requirements (see Applicability of the GDPR and National Law). Hong Kong entities (which includes Hong Kong companies, organizations and affiliates of US companies) subject to the GDPR must comply with additional data protection obligations than the Ordinance requires

Failing to comply with the GDPR carries substantial penalties and may result in fines of up to EUR20 million or 4% of the entity's total worldwide annual revenue for the preceding financial year, whichever is higher (Article 83(5), GDPR).

This Chart compares important topics under the Ordinance and the GDPR, such as:

- Definitions of personal data and sensitive personal data.
- Appointing an EU representative.
- Appointing data protection officers.
- Completing data protection impact assessments.
- Maintaining processing records.
- Legal justifications for processing personal data and special categories of personal data, also called sensitive personal data.

- Consent of data subjects.
- Data subject rights, such as notice, access, correction, erasure, and objection.
- Data security requirements.
- Breach notification requirements.
- Cross-border personal data transfers.

This Chart does not cover every topic addressed by these laws or provide detailed guidance on necessary steps to comply with the laws. For a more detailed comparison of the GDPR and Hong Kong Ordinance, see Practice Note, GDPR Compliance for Hong Kong Businesses.

Applicability of the GDPR and National Law

The Hong Kong Office of the Privacy Commissioner for Personal Data (Commissioner) has issued guidance on the GDPR, including a publication (in Chinese and English) which discusses the GDPR's potential applicability to Hong Kong organizations. For more information, see the Commissioner's website.

The European Data Protection Board (EDPB) has also issued Guidelines on the territorial scope of the GDPR (Article 3) (EDPB 3/2018) (November 12, 2019). For more on the GDPR's applicability, see Practice Note, Determining the Applicability of the GDPR.

The GDPR introduced a single legal framework across the EU. However, several GDPR provisions allow EU member states to enact national legislation specifying, restricting, or expanding the scope of some of the GDPR's requirements. Non-EU-based organizations may be subject to requirements under multiple national laws. National laws implementing the GDPR are outside the scope of this Chart. For more, see Practice Note, Determining the Applicability of the GDPR: Applicability of EU Member State Laws and the GDPR National Implementation Legislation Toolkit.

GDPR and Hong Kong Ordinance Comparison Chart

	GDPR	Hong Kong Ordinance	Comparison
Scope	Obligations apply to controllers (Article 4(7)) and processors (Article 4(8)) that process personal data: • Wholly or partly by automated means. • Other than by automated means when the personal data forms part	Obligations apply to data users (concept similar to controller) when collecting, using, or handling personal data (Section 2).	GDPR is broader in scope because it obligates both controllers and processors. The Ordinance does not impose direct obligations on data processors.

	of or is intended to form part of a filing system. (Article 2(1).)		

Extra-territorial application	Applies to:
	
	• Controllers and processors that process personal data in the context of the activities of an EU establishment, regardless of whether the data processing takes place in the EU (Article 3(1)).
	
	• Controllers and processors not established in the EU that process personal data about data subjects in the EU when the processing activities relate to:
	  • offering goods or services to EU data subjects in the EU, regardless of whether they require payment; or
	  • monitoring their behavior that takes place in the EU.
	
	(Article 3(2).)
		The current legal framework only applies to data users in Hong Kong, regardless of where the data user's servers are located or where the data subjects are based. Ordinance Section 33, which is not yet in force, will change this standard. For more, see Practice Note, GDPR Compliance for Hong Kong Businesses: Cross-Border Data Transfers: Ordinance Requirements.	Unlike the Ordinance, the GDPR has an extraterritorial reach and applies to controllers and processors outside the EU.

Definition of personal data	Defines "personal data" as any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one that can be identified, directly or indirectly, by reference to an identifier, such as name,	Any data relating directly or indirectly to a living individual, or from which it is possible to directly or indirectly identify an individual, when the data user holds the personal data in a form that permits access to or	GDPR and Ordinance include similarly broad definitions of personal data.

	ID number, location data, or online identifier (Article 4(1)).	processing of the data (Section 2).	
Definition of sensitive personal data	Defines "special categories of personal data" (considered sensitive) to include: • Racial or ethnic origin. • Political opinions. • Religious or philosophical beliefs. • Trade union membership. • Health data and data about sex life or sexual orientation. • Genetic and biometric data. (Article 9(1).) Includes personal data that may indirectly reveal special categories of personal data concerning an individual (see Case C-184/20: OT v Vyriausioji tarnybinės etikos komisija (Chief Official Ethics Commission, Lithuania)). The GDPR also regulates processing personal data related to criminal convictions or offenses (Article 10).	Does not define sensitive personal data. The Commissioner has published several guidelines indicating that data users must treat certain types of personal data seen as particularly sensitive with extra caution, for example, Hong Kong Identity Card numbers and biometric data.	GDPR expressly protects certain sensitive categories of personal data and restricts processing unless an exception applies. The GDPR also restricts processing criminal conviction or offense data.

Registration before processing	Not required unless an EU member state law implementing the GDPR requires registration under specific circumstances.	Not required unless in a special class of data users identified by the Commissioner in a notice in the Gazette (Section 14).	GDPR and Ordinance generally do not require registration.
Processing principles	The six principles that govern personal data processing include: • Lawfulness, fairness, and transparency. • Purpose limitation. • Data minimization. • Accuracy. • Storage limitation. • Integrity and confidentiality. Controllers must: • Comply with the six principles when processing personal data. • Demonstrate compliance with all six of the principles. (Article 5.)	The six principles that govern personal data processing include: • Purpose and manner of collection which must be lawful, fair, and transparent. • Accuracy and storage limitation. • Use requirements and limitations. • Personal data security. • Notice of data user's policies, the categories of personal data processed, and the purposes of processing. • Access. (Schedule 1.)	GDPR and Ordinance principles are similar.
EU representative	Non-EU-based organizations engaging in certain activities must designate an EU representative in	Not required.	GDPR includes requirements that do not exist in the Ordinance.

	writing, subject to limited exceptions (Article 27(1)).		
Data protection officer (DPO)	Required in certain circumstances (Article 37).	Not required, however entities subject to the Protection of Critical Infrastructures (Computer Systems) Bill (PCICS Bill) may be required to appoint a DPO in certain circumstances. The PCICS Bill is effective from 1 January 2026.	GDPR includes requirements that do not exist in the Ordinance.
Data protection impact assessment	Required for certain types of high-risk processing, such as: • New technologies. • Automated processing, including profiling, on which decisions are based that produces legal or other similarly significant effects for a data subject. • Large scale processing of special categories of personal data or criminal conviction and offenses data. • Large scale, systematic monitoring of a publicly accessible area. (Article 35.) Requires consultation with data protection authorities if assessment reveals high risks to data subject in the	Not required. The Commissioner has issued guidance that encourages data users to carry out a privacy impact assessment as a best practice.	GDPR includes requirements that do not exist in the Ordinance.

	absence of risk mitigation measures taken by the controller (Article 36).		
Records of processing activities	Controller and processor must maintain a record of processing activities, subject to limited exceptions (Article 30).	Not required.	GDPR includes requirements that do not exist in the Ordinance.
Accountability	Controllers must comply with the data processing principles (Article 5(1)) and demonstrate compliance (Article 5(2)).	Not required. Data users subject to the PCICS Bill may be subject to fines for non-compliance.	GDPR includes a specific accountability requirement while the Ordinance does not.
Conditions for processing personal data	Requires a legal basis to process personal data (Article 6).	Does not require a legal basis to process personal data.	GDPR has stricter requirements for processing personal data.
Consent	Consent is one legal basis for processing personal data recognized by the GDPR (Article 6(1)). Consent must satisfy specific requirements, including that it be freely given, specific, informed, and unambiguous and the controller must be able to show it obtained consent (Articles 4(11) and 7). Implied consent and opt-out consent are not valid (Article 4(11)). Certain types of personal data processing require	Not required, except in limited circumstances (Section 35(C)(2) and Principle 3, Schedule 1). When required, consent must generally be express and voluntary, it cannot be implied or inferred (Principle 3, Schedule 1). Data users must obtain consent before using personal data for direct marketing purposes by requesting that a data subject take some action to indicate that it either:	GDPR includes more robust consent requirements than the Ordinance. Consent is only one basis for processing personal data under the GDPR. The GDPR does not require consent if another legal basis for processing applies.

	explicit consent including when relying on consent to: • Process special categories of personal data. • Transfer personal data cross-border. • Make decisions based on automated personal data processing. (Articles 9, 22, and 49.)	• Consents to the use of its data for direct marketing purposes, such as by ticking a box or clicking a button. • Has no objection to this use, such as by not ticking a clear and prominent checkbox that indicates the data subject does not agree to receive direct marketing emails. (Sections 35A(1), 35C, and 35E, Ordinance; and see Commissioner's New Guidance on Direct Marketing, at 10 to 11.)	
Conditions for processing special categories of personal data (sensitive data) and criminal convictions and offense data	Prohibits processing special categories of personal data unless an exception applies (Article 9). When relying on consent to process special categories of personal data, the controller must obtain explicit consent (Article 9(2)(a)). The GDPR also restricts processing personal data relating to criminal convictions and offenses unless certain conditions apply (Article 10, GDPR).	Does not address sensitive personal data, but regulator guidelines suggest special treatment of certain categories of data such as biometric data, health records, and personal identifiers.	GDPR includes express prohibitions and restrictions on processing special categories of personal data and criminal conviction and offense data that do not exist in the Ordinance.
Child consent	Parental consent required for children under 16.	Parental consent not required except in	GDPR has specific requirements for

	However, EU member states can lower the age of consent to a minimum of 13 (see GDPR Age of Child Consent Chart (EEA): Overview). (Article 8.)	the limited situations that require consent. Ordinance does not set a minimum age for consent.	obtaining child consent while the general consent requirements apply under the Ordinance to minors.
Direct marketing	Permitted if the controller satisfies the GDPR's requirements for lawfully processing personal data and handling data subject objections to direct marketing (Articles 6 and 21).	Data users must provide notice and obtain consent before using personal data for direct marketing purposes by requesting that a data subject take some action to indicate that it either: • Consents to the use of its data for direct marketing purposes, such as by ticking a box or clicking a button. • Has no objection to this use, such as by not ticking a clear and prominent checkbox that indicates the data subject does not agree to receive direct marketing emails. (Sections 35A(1), 35C, and 35E, Ordinance; and see Commissioner's New Guidance on Direct Marketing, at 10 to 11.)	Ordinance includes detailed direct marketing requirements. GDPR includes requirements for lawful processing and handling datasubjects' objections to direct marketing.
Information right	Information right with broad content requirements (Articles 12 to 14). For more on the GDPR's notice requirements,	Information right with more limited content requirements (Schedule 1, Section 1(3)).	GDPR is broader and requires a more detailed and comprehensive privacy notice.

	see Practice Note, Complying with the GDPR's Transparency Obligation to Data Subjects.		
Access rights	Right to access personal data, obtain certain information about the processing, and receive a copy of certain personal data on request (Articles 12 and 15).	Right to access personal data and receive a copy (Section 18 and Principle 6, Schedule 1).	GDPR and Ordinance provide similar access rights.
Erasure right, also called "right to be forgotten"	Express right to request erasure of personal data in specific circumstances (Article 17).	Does not provide data subjects with an explicit erasure right. However, it requires data users to ensure they do not retain personal data for longer than necessary to fulfill the original collection purpose (Principle 2(2), Schedule 1).	GDPR provides data subjects with greater right.
Rectification right	Right to obtain rectification without undue delay or to complete incomplete personal data (Article 16).	Right to obtain correction within 40 days (Section 22).	GDPR and Ordinance are similar but include different timing requirements.
Objection right	Right to object to data processing in certain circumstances (Article 21).	Not addressed.	GDPR includes an objection right while the Ordinance does not.
Restriction right	Right to restrict data processing in certain circumstances, such as when a data subject contests the data's accuracy or while a processing objection is pending (Article 18).	Not addressed.	GDPR includes a restriction right while the Ordinance does not.

Data portability right	Right to data portability, which includes the right to: • Receive a copy of certain personal data from the controller in a commonly used and machine-readable format and store it for further personal use on a private device. • Transmit certain personal data to another controller. • Have certain personal data transmitted directly from one controller to another where technically possible. (Article 20(1) and (2).)	Not addressed.	GDPR includes a data portability right while the Ordinance does not.
Automated decision-making	Right not to be subject to a decision based solely on automated processing, including profiling, which has legal or other significant effects on the data subject, subject to certain exceptions (Article 22).	Prohibits the use of automated data processing that amounts to a "matching" procedure except in limited circumstances (Section 30).	GDPR provides data subjects with greater rights to not be subject to certain automated decisions. Ordinance only addresses the use of automated data processing that amounts to a "matching" procedure and allows it under limited circumstances.
Data security requirements	Requires appropriate technical and organizational security measures to ensure a level of security appropriate to	Requires data users to take practical steps to protect personal data against unauthorized or accidental access, processing, erasure,	GDPR and Ordinance both require security measures appropriate to the risk.

	the risk (Articles 25 and 32).	loss, or use (Principle 4, Schedule 1). Data users subject to the PCICS Bill may be required to implement certain data security requirements.	GDPR includes more detailed requirements on data protection by design and by default.
Data protection by design and default	Required (Article 25).	Not required.	GDPR includes requirements that do not exist in the Ordinance.
Data breach notification	Controllers experiencing a data breach must notify: • The relevant supervisory authority no later than 72 hours after the breach, unless the breach is unlikely to pose a risk of harm (Article 33). • The data subject without undue delay if the breach poses a high risk of harm (Article 34). The GDPR requires processors to notify the controller without undue delay when they become aware of a personal data breach (Article 33(2)).	Not required, but Commissioner recommends that organizations notify regulators and individuals in certain circumstances (Guidance on Data Breach Handling and the Giving of Breach Notifications, at 5 and 7). Data users subject to the PCICS Bill may be required to provide data breach notifications.	GDPR includes requirements that do not exist in the Ordinance.
Data processor contracts	A contract or other legal act that includes specified terms must govern processor relationships (Article 28(3)).	Execution of data processing agreements not explicitly required. However, the Commissioner strongly recommends the use of contracts in its guidelines (see PCPD: Outsourcing	Processor contracts under the GDPR must include specific terms, some of which vary from the recommended terms under Hong Kong's guidance.

		the Processing of Personal Data to Data Processors).	
Certifications and codes of conduct	Recognizes codes of conduct and certifications as mechanisms to demonstrate compliance with the GDPR's requirements (Articles 40 and 42).	Not formally recognized as a compliance or accountability tool.	GDPR includes provisions on codes of conduct and certifications that do not exist in the Ordinance.
Cross-border transfers	Prohibits personal data transfers outside of the EU unless an exception applies (for example, when the recipient country ensures an adequate level of protection, or the transfer is subject to appropriate safeguards) (Articles 44 to 50).	Restricted by Section 33, but not yet effective and no date set for implementation.	GDPR restricts cross-border transfers unless certain conditions are satisfied. Similar Ordinance provisions are not yet in effect.

END OF DOCUMENT