GDPR Compliance for Hong Kong Businesses

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 Practice Note discussing the key differences between the Hong Kong Personal Data (Privacy) Ordinance (Cap 486) and the EU General Data Protection Regulation (GDPR). This Note discusses the GDPR's applicability to Hong Kong organizations. This Note also discusses additional measures that Hong Kong organizations must take to comply with the GDPR.

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) explicitly requires non-EU based entities engaging in certain EU-related activities to comply with its requirements.

In Hong Kong, the Personal Data (Privacy) Ordinance (Cap 486) (Ordinance) regulates personal data collection and processing.

However, compliance with the Ordinance does not mean that a Hong Kong entity (which includes Hong Kong companies and organizations) also complies with the GDPR because it includes several different requirements. For example, the GDPR includes an accountability principle, which creates an obligation to demonstrate compliance with its requirements. The GDPR also includes expanded data subject rights and a data breach notification requirement. Hong Kong entities that are subject to the GDPR must review the GDPR's applicability provisions to determine whether it applies to their activities.

Hong Kong entities subject to the GDPR face greater data protection obligations than the Ordinance requires. Failing to comply with the GDPR also 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). GDPR enforcement is robust therefore it is important for Hong Kong entities to ensure compliance. For more on enforcement and sanctions under the GDPR, see Practice Note, Enforcement, Sanctions, and Remedies under the GDPR.

This Note provides an overview of the key differences between Hong Kong's Ordinance and the GDPR. It also discusses the GDPR's applicability to non-EU entities and steps that Hong Kong entities should take to comply with the GDPR. This Note specifically discusses:

- The GDPR's extra-territorial application.
- The requirement for non-EU-established entities to appoint an EU representative.
- Obligations applicable to controllers and processors.
- The GDPR's accountability principle and the obligation to demonstrate compliance.
- Compliance measures not required by the Hong Kong Ordinance.

- Consent requirements.
- Data breach notification requirements.
- A comparison of data subject rights under the GDPR and the Ordinance.
- Cross-border data transfer restrictions.

EU General Data Protection Regulation (GDPR)

The GDPR applies to the processing of personal data by:

- Controllers and processors established in the EU (see Controllers and Processors Defined and EU Establishments).
- Certain non-EU-established controllers and processors (see Extra-Territorial Application).

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 entities. 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) (Territorial Scope Guidelines).

EU Establishments

A Hong Kong entity (whether a controller or processor) with an establishment in the EU must comply with the GDPR when processing personal data in the context of that establishment, regardless of the nationality of the data subjects or even if the entity processes the personal data outside the EU (Article 3(1) and Recital 22, GDPR). For example, the GDPR may apply to a Hong Kong-based entity if it both:

- Has an EU-established subsidiary, affiliate, or branch.
- Processes personal data in the context of that establishment.

Lack of a branch or subsidiary in the EU does not preclude a non-EU entity from having an EU establishment. In some circumstances, having a single employee or agent in the EU may subject the Hong Kong entity (whether as a controller or processor) to the GDPR under Article 3(1). (Territorial Scope Guidelines, at 6.) The GDPR also applies to entities (whether as controllers or processors) with an EU establishment that process personal data in the context of that establishment, even if data subjects are located outside the EU (Territorial Scope Guidelines, at 7 to 9).

To determine whether a non-EU entity processes personal data in the context of an EU establishment, the EDPB recommends identifying links between the non-EU entity's processing activities and the activities of the EU establishment. These links are key to determining whether the GDPR applies to the processing (Territorial Scope Guidelines, at 6 to 8).

For more on determining whether the GDPR applies based on an EU establishment, see Practice Note, Determining the Applicability of the GDPR : Applicability Based on an EU Establishment and the Territorial Scope Guidelines.

Extra-Territorial Application

The GDPR extends to controllers and processors not established in the EU when they engage in certain activities affecting EU data subjects. Hong Kong entities with an existing EU customer base must comply with the GDPR. Entities without an existing customer base must comply if they target or intend to target individuals in the EU.

The GDPR applies to personal data processing conducted by a Hong Kong controller or processor with no EU establishment that relates to:

- Offering goods or services to data subjects in the EU, regardless of whether the controller or processor requires payment.
- Monitoring data subjects' behavior that takes place in the EU.

(Article 3(2), GDPR.)

The Territorial Scope Guidelines recommend that entities first consider whether data subjects are located in the EU and second, whether the processing relates to offering goods or services or monitoring behavior (Territorial Scope Guidelines, at 14).

Accessibility of a non-EU-established controller's or processor's website by an EU data subject or access to the email address or other contact details of the non-EU-established controller or processor from the EU does not by itself mean that the GDPR applies (Recital 23, GDPR).

Entities may show intent to attract EU data subjects as customers by, for example:

- Referring to the EU or at least one EU member state by name when referencing the goods or services.
- Offering goods or services in an EU language or currency.
- Allowing EU data subjects to place orders in the local language.
- Offering delivery in EU member states.
- Directing marketing campaigns at an EU member state audience.
- Using country-specific top-level domains or the top-level domain ".eu."

(Territorial Scope Guidelines, at 17 to 18.)

Hong Kong entities that do not offer goods or services to EU data subjects may still fall within the GDPR's scope if they monitor data subjects' behavior that takes place in the EU. Monitoring under GDPR Article 3(2)(b) may encompass a broad range of activities, for example:

- Behavioral advertising.
- Geo-location tracking for marketing purposes.
- Data collection or tracking through wearables and other smart devices.
- Web analytics, cookies, and other online tracking.
- Online personalized diet and health analytics services.
- Closed circuit television camera use.
- Market surveys and other behavioral studies based on profiling.
- Data gathering or regular reporting on individuals' health status.

(Territorial Scope Guidelines, at 20.)

For more on determining whether the GDPR applies to entities without an EU establishment, see Practice Note, Determining the Applicability of the GDPR: Applicability Based on an EU Establishment and the Territorial Scope Guidelines.

EU Representative

Hong Kong entities subject to the GDPR but not established in the EU, must designate an EU representative in writing, subject to limited exceptions (Article 27(1), GDPR). The EU representative is a natural or legal person established in the EU representing the Hong Kong entity (whether controller or processor) concerning its GDPR obligations (Article 4(17), GDPR). The EU representative must:

- Maintain an establishment in an EU member state where the Hong Kong entity's data subjects are located.
- Be empowered to address all issues relating to data processing raised by supervisory authorities and data subjects, in addition to or instead of the Hong Kong entity (controller or processor).

(Articles 27(3), (4), GDPR.)

The requirement to appoint an EU representative does not apply when:

- The processing:

- is occasional;
- excludes large-scale processing of special categories of personal data (see Personal Data and Sensitive Personal Data Defined) or criminal conviction or offense data; and
- is unlikely to result in a risk to the data subject's rights and freedoms, considering the nature, context, scope, and purposes of processing.

- The controller is a public authority or body.

(Article 27(2)(a), GDPR.)

For more on the EU representative's obligations under the GDPR, see Territorial Scope Guidelines, at 23 to 28. For more on the key requirements and considerations when appointing a data protection representative, see Practice Notes, Appointing a data protection representative in EU or UK (UK) and Appointing a representative in the EEA and the UK: FAQs.

Controllers and Processors Defined

The GDPR defines:

- A controller as the natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of processing personal data (Article 4(7), GDPR).
- A processor as the natural or legal person, public authority, agency, or other body that processes personal data on a controller's behalf (Article 4(8), GDPR).

The EDPB has issued Guidelines on the concepts of controller and processor in the GDPR (EDPB 07/2020) (July 7, 2020). For a checklist to determine whether a party is a controller or processor under the GDPR, see Controller or processor? (UK and EU): checklist. The GDPR imposes obligations on controllers and processors.

The Ordinance adopts the term "data users" to describe a concept similar to the GDPR's controller definition. It defines a data user as a person who, either alone or jointly with other persons, controls the collection, holding, processing, or use of personal data (Section 2, Part 1, Ordinance). "Processor" under the Ordinance means a person who processes personal data on another person's behalf and who does not process the data for the person's own purposes (Principle 2(4), Ordinance).

Unlike the GDPR, the Ordinance does not impose direct obligations on processors.

Hong Kong entities subject to the GDPR must determine whether they act as a controller or processor to understand which GDPR obligations apply. Entities which act solely as processors must review the GDPR's applicability provisions and requirements. For more on processor obligations, see Processor Obligations.

Personal Data and Sensitive Personal Data Defined

The GDPR broadly defines personal data to include any information relating to an identified or identifiable natural person (data subject). Personal data includes location data and online identifiers (Article 4(1), GDPR). The Ordinance includes a similarly broad definition of personal data (Section 2, Part 1, Ordinance).

In contrast to the GDPR, the Ordinance does not identify certain categories of personal data as sensitive or apply more stringent protections to some categories of personal data. However, while the Ordinance establishes the same legal requirements for all categories of personal data, the personal data's nature or sensitivity can affect what the law considers reasonable security or appropriate use under the circumstances. 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.

The GDPR considers certain categories of personal data more sensitive and defines special categories of personal data as:

- 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), GDPR.)

Special categories of personal data includes personal data that may indirectly reveal sensitive information concerning an individual (Case C-184/20: OT v Vyriausioji tarnybin#s etikos komisija (Chief Official Ethics Commission, Lithuania); see Legal Update, Information indirectly disclosing sexual orientation is special category personal data (ECJ)).

The GDPR prohibits processing special categories of personal data unless an exception applies. The GDPR also restricts processing criminal conviction and offense data (Article 10, GDPR).For more on processing special categories of personal data, see Justifications for Processing Special Categories of Personal Data and Practice Note, Overview of EU General Data Protection Regulation: Special Categories of Personal Data.

Hong Kong entities that process special categories of personal data or criminal conviction and offense data about data subjects in the EU must ensure that they meet the GDPR's additional requirements for processing this data.

Principles Governing Personal Data Processing

Similar principles govern personal data processing under the GDPR and the Ordinance. The six principles governing personal data processing under the GDPR are:

- **Lawfulness, fairness, and transparency**.

- **Purpose limitation**, which means that an entity should:
    - only collect personal data for specified, explicit, and legitimate purposes; and
    - not process the personal data in a manner that is incompatible with those purposes, except under limited circumstances.
- **Data minimization**, which means that personal data should be:
    - adequate;
    - relevant; and
    - limited to what is necessary for processing.
- **Accuracy**, which means that personal data must be:
    - accurate and kept up-to-date; and
    - corrected or deleted without delay when inaccurate.
- **Storage limitation**, which requires that the entity keep personal data in identifiable form only for as long as necessary to fulfill the purposes that it collected it for, subject to limited exceptions.
- **Integrity and confidentiality**, which requires that the entity secures personal data by appropriate technical and organizational measures against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

(Article 5(1), GDPR.)

For more on processing personal data under the GDPR, see Practice Note, Overview of EU General Data Protection Regulation. For more on processing personal data under Hong Kong law, see Country Q&A, Data Protection in Hong Kong: Overview.

Applicability of EU Member State Laws

The GDPR introduced a single legal framework across EU member states. However, several GDPR provisions allow EU member states to enact national legislation specifying, restricting, or expanding the scope of certain GDPR requirements. As a result, entities may face inconsistent requirements from one EU member state to the next. For information on the permitted EU member state variations under the GDPR, see Practice Note, GDPR Derogations and Exemptions: Overview.

Hong Kong entities handling EU personal data may be subject to multiple national laws if they:

- Have multiple EU establishments.
- Are a non-EU-established entity that offers goods or services to or monitors data subjects' behavior that takes place in multiple EU member states.

Entities subject to the GDPR must review the territorial scope provisions in the relevant EU member state laws to determine which laws apply. For more on EU member states' implementation of the GDPR, see GDPR National Implementation Legislation Toolkit.

The requirements of the national laws implementing the GDPR are outside the scope of this Note. However, Hong Kong entities should review and comply with the relevant laws' requirements in addition to the GDPR.

Data Privacy Governance

Entities subject to the GDPR must:

- Assess how the requirements affect them.
- Determine what steps they must take to comply, which may include auditing existing data protection practices and updating procedures and policies.

Entities should also consider ways to leverage existing practices already in place to comply with the Ordinance.

Hong Kong entities may need to adjust their existing practices to comply with the GDPR's stricter standard for processing EU personal data. Some entities may choose to apply the GDPR's higher standard to all their data collection and processing activities. Other entities may adopt a regional approach and only apply the GDPR's requirements to their processing activities relating to EU personal data.

Accountability and Demonstrating Compliance

The GDPR incorporates a principle of accountability and requires controllers to both:

- Comply with the six principles when processing personal data (Article 5(1), GDPR; see Principles Governing Personal Data Processing).
- Demonstrate compliance with all six of the principles (Article 5(2), GDPR).

The GDPR also requires controllers to implement appropriate technical and organizational measures to ensure and be able to demonstrate that their processing complies with the GDPR's requirements (Article 24(1), GDPR). Meeting the GDPR's accountability requirement means doing more than just establishing data protection policies and procedures. The accountability principle effectively requires a controller to implement a formal data protection compliance program (see Practice Note, Demonstrating Compliance with the GDPR: Accountability and Demonstrating Compliance).

While the Ordinance does not explicitly include the accountability principle, the Commissioner advocates the adoption of a privacy compliance program. However, the privacy compliance programs established by Hong Kong entities may not satisfy the GDPR's requirements. Entities should audit existing compliance programs for compatibility with the GDPR and assess compliance gaps (see Implementing the General Data Protection Regulation (GDPR) Checklist: Align the Business's Personal Data Collection and Processing Practices with GDPR's Requirements).

Accountability for Processors

The accountability principle under GDPR Articles 5 and 24 expressly applies to controllers. However, in practice, the GDPR obligations imposed directly on processors or indirectly passed on by controllers also subject processors to certain accountability requirements. For more information on processors' accountability, see Processors and Practice Note, Demonstrating Compliance with the GDPR: Accountability for Processors.

Compliance Measures Not Required by Hong Kong's Ordinance

Hong Kong entities subject to the GDPR likely need to revise their compliance programs to address certain aspects of GDPR compliance not found in the Ordinance, for example, requirements to:

- **Appoint data protection officers** (DPO) (Article 37, GDPR). For more on when the GDPR requires controllers and processors to appoint a DPO and the DPO's obligations, see:
    - Practice Note, Data Protection Officers Under the GDPR.
    - Standard Document, Data protection officer: role specification (EU/UK).
    - Implementing the General Data Protection Regulation (GDPR) Checklist: Appoint Data Protection Officer (DPO) or Other Data Protection Leader.
    - Country Q&A, Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: EU.
    - Article 29 Working Party: Guidelines on Data Protection Officers (DPOs) (WP243) April 5, 2018).
- **Implement data protection by design and by default** (Article 25, GDPR). For more on this requirement, see Practice Notes, Overview of EU General Data Protection Regulation: Data Protection by Design and by Default and Implementing the General Data Protection Regulation (GDPR) Checklist: Data Protection by Design and Default.
- **Conduct a data protection impact assessment (DPIA) for certain types of high-risk processing** (Article 35, GDPR). For more on when the GDPR requires a DPIA, see Practice Note, Data Protection Impact Assessments Under the GDPR.
- **Maintain a record of processing activities** (Article 30, GDPR). This requirement does not apply when the entity employs fewer than 250 people unless the processing:
    - is likely to result in a risk to the data subject's rights and freedoms;

- is not occasional; or
- includes special categories of personal data or criminal conviction or offense data.

For more on what to include in the record of processing activities, see Practice Notes, Demonstrating Compliance with the GDPR: Record of Processing Activities, Data Mapping and GDPR Recordkeeping Obligations, and Standard Document, Record of Processing Activities Under Article 30 (GDPR).

For more on developing a privacy compliance program, see Practice Note, Developing a Privacy Compliance Program. For more on the GDPR's obligation to demonstrate compliance and how to comply with this obligation, see Practice Note, Demonstrating Compliance with the GDPR.

Certifications and Codes of Conduct

The GDPR explicitly recognizes codes of conduct (Article 40) and certifications (Article 42) as mechanisms to demonstrate compliance with the GDPR's requirements. Participation in a code of conduct or certification scheme is voluntary. The Ordinance does not formally recognize certification or privacy seal mechanisms as a compliance or accountability tool.

Before codes of conduct and certifications can provide reliable evidence of GDPR compliance, clear rules and requirements for certification must be in place. The GDPR provides for the development of these rules.

For more on codes of conduct and certification mechanisms, see Practice Note, Overview of EU General Data Protection Regulation: Approved Codes of Conduct and Approved Certification Mechanisms and GDPR European Data Protection Board Guidance Tracker.

Conditions for Processing

The Ordinance does not require consent to process personal data, except under limited circumstances (see Ordinance Consent Requirements). It also does not require a data user to have a legal basis to process personal data.

In contrast, the GDPR:

- Requires controllers to have a legal basis for processing.
- Recognizes consent as one legal basis permitting processing.

(See Practice Note, Consent under the GDPR.)

Some EU supervisory authorities have questioned the validity of processing based on consent in certain circumstances, such as in an employer/employee relationship. Entities should rely on another legal basis to process personal data whenever possible unless applicable law requires consent.

Other legal bases under the GDPR that permit personal data processing include when processing is necessary for:

- Performing a contract with the data subject.
- Complying with a legal obligation.
- Protecting the data subject's vital interests.
- Performing a task carried out in the public interest.
- Pursuing the controller's or a third party's legitimate interests, except where the data subject's interests or fundamental rights and freedoms override the controller's or third party's interests.

(Article 6(1), GDPR; see Practice Note, Overview of EU General Data Protection Regulation: Lawful Processing.)

Hong Kong entities subject to the GDPR should identify and document their legal basis for processing EU personal data (see Practice Note, Demonstrating Compliance with the GDPR: Lawfulness of Processing).

Justifications for Processing Special Categories of Personal Data

The GDPR prohibits entities from processing special categories of personal data unless an exception applies, including when:

- The data subject explicitly consents to the processing.
- The processing relates to personal data made public by the data subject.
- The processing relates to the legitimate interests of certain non-profit organizations.
- The processing is necessary for:
    - carrying out the controller's rights and obligations in the field of employment law, social security, and social protection;
    - protecting the vital interests of the data subject when the controller cannot obtain consent;
    - establishing, exercising, or defending legal claims;
    - reasons of substantial public interest;
    - purposes of preventive or occupational medicine, assessing an employee's working capacity, medical diagnosis, or for the provision of health or social care or treatment;
    - reasons of public interest in the area of public health;

- archiving in the public interest; or
- scientific, historical research, or statistical purposes.

(Article 9, GDPR.)

The GDPR also limits personal data processing relating to criminal convictions and offenses to certain circumstances, including when applicable law authorizes the processing and provides for appropriate safeguards for data subjects' rights and freedoms (Article 10, GDPR).

Hong Kong entities must ensure they have a legal basis under the GDPR to process EU data subjects' special categories of personal data. For more information, see Practice Note, Overview of EU General Data Protection Regulation: Processing Special Categories of Personal Data.

Consent

Ordinance Consent Requirements

The Ordinance only requires prescribed consent to process personal data under limited circumstances, for example, when the entity:

- Wants to use previously collected personal data for a new or different purpose that it did not disclose to the data subject and that is not directly related to the original purpose of use (Principle 3, Ordinance).
- Wants to use personal data for direct marketing purposes (Sections 35C(2) and 35(J), Ordinance).
- Wants to transfer personal data to a third party and the entity did not disclose the transferee in the original privacy notice (see Notice).
- Intends to use automated data processing that amounts to a matching procedure (see Automated Decision-Making Objection).

Prescribed consent:

- Means express consent given voluntarily.
- Cannot be implied or inferred.
- May be verbal or written and given in person, in paper form, or online.

(Principle 3, Ordinance; Paragraphs 7.59 and 7.60, Personal Data (Privacy) Law in Hong Kong: A Practical Guide on Compliance.)

Bundled consent is not a valid form of consent according to the Commissioner (PCPD: New Guidance on Direct Marketing, at 7 to 9). Bundled consent occurs, for example, when a data user requires data subjects to consent to an unrelated use of their personal data, such as direct marketing, as a condition of obtaining a product or service.

Prescribed consent may be subsequently withdrawn by notice in writing to the data user (Part 1, Section 2(3), Ordinance).

For more on obtaining consent under the Ordinance, see Country Q&A, Data Protection in Hong Kong: Overview: Question 9.

GDPR Consent Requirements

The GDPR imposes stringent requirements on obtaining valid consent and requires consent to be:

- Freely given.
- Specific.
- Informed.
- Unambiguous.

(Article 4(11), GDPR.)

A data subject's silence, inactivity, or failure to uncheck a pre-checked box does not indicate consent. Implied consent and opt-out consent are not valid (Article 4(11), GDPR). The GDPR also requires that written requests for consent be:

- Clearly distinguishable from other matters. Bundled consents are not valid.
- Intelligible.
- Easily accessible.
- Written using clear and plain language.

(Article 7(2), GDPR.)

To obtain freely given consent, the controller must not condition the performance of a contract, including providing a service, on the data subject's consent for processing unrelated to or unnecessary for the contract's performance or service's provision (Article 7(4), GDPR).

Certain types of personal data processing under the GDPR require 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, GDPR.)

The GDPR does not define explicit consent. However, the EDPB's (formerly the Article 29 Working Party) Guidelines on Consent under Regulation 2016/679 (WP259) (April 10, 2018) (GDPR Consent Guidelines) describe explicit consent similarly to express consent under the Ordinance, including confirming consent in an oral or written statement, or via online or digital methods, including electronic forms, emails, or electronic signatures (GDPR Consent Guidelines, at 20 to 21).

Like consent under the Ordinance, the GDPR permits data subjects to withdraw consent at any time (Article 7(3), GDPR). For more on the GDPR's consent requirements and obtaining valid consent, see Practice Note, Consent Under the GDPR: Using Consent to Process Personal Data in the EEA, Best Practices When Using Consent to Process Personal Data and the GDPR Consent Guidelines.

Satisfying the GDPR's requirements for valid consent is difficult and may often be impractical. Due to the heightened requirements for obtaining valid consent and the data subject's right to withdraw consent at any time, entities are encouraged to rely on one of the other legal bases in GDPR Article 6 to process personal data (see Conditions for Processing).

Consent from Minors

Under the GDPR, when an online service (called an "information society service" in the GDPR) is offered directly to a child, the child can only consent to the processing of their personal data if they are at least 16 years old. If the child is under 16 years old, parental consent is required. The GDPR allows EU member states to lower the age of consent to a minimum age of 13. Controllers must use reasonable efforts to verify parental consent considering available technology (Article 8, GDPR.)

Under the Ordinance, a person who has parental responsibility may give prescribed consent on behalf of a minor under the age of 18 (see Part 2, Section 3, Interpretation and General Clauses Ordinance (Cap 1)), if both:

- The minor is incapable of understanding the proposed purpose and deciding whether to give the prescribed consent.
- The parent has reasonable grounds for believing that the use of the personal data for the proposed purpose is clearly in the minor's interest.

A similar rule applies to mentally incapacitated persons and persons incapable of managing their own affairs. (Principle 3(2)(a), Ordinance.)

Hong Kong entities that collect personal data from children younger than the age of consent set by applicable EU member state law must comply with the GDPR's consent requirements for minors. For more on the requirements for obtaining consent from minors, see Practice Note, Consent Under the GDPR: Child Consent and GDPR Age of Child Consent Chart (EEA): Overview.

Processors

Processor Obligations

The Ordinance does not directly regulate or impose liability on processors. Instead, the Ordinance requires data users to implement contractual or other means with third-party processors to protect personal data in the processor's possession, including to:

- Prevent unauthorized or accidental access, processing, erasure, loss, or use of the personal data transferred.
- Ensure that the processor only keeps personal data for as long as necessary to fulfill the purposes of the processing.

(Principles 2(3) and 4(2), Ordinance.)

In contrast, the GDPR imposes liability and direct obligations on processors to:

- Process personal data only according to the controller's instructions (Article 29, GDPR).
- Maintain a record of data processing activities (Article 30(2), GDPR).
- Appoint a DPO in certain circumstances (Article 37, GDPR).
- Implement appropriate technical and organizational security measures (Article 32, GDPR).
- Have written controller authorization before engaging subcontractors under GDPR Article 28(2) and pass obligations down to any processors it engages through contracts (Article 28(4), GDPR).
- Notify the controller of any security breach without undue delay (Article 33(2), GDPR; see Data Breach Notification).
- Appoint an EU representative when the processor is not located in the EU, subject to certain limited exceptions (Article 27, GDPR; see EU Representative).
- Only transfer personal data internationally under GDPR Article 44, which requires the processor to have a compliant data transfer mechanism (see Cross-Border Data Transfers).
- Make available to the controller all information for the controller to demonstrate compliance with its obligations under GDPR Article 28 (Article 28(3)(h), GDPR).

Processors face direct sanctions for GDPR noncompliance. For more on processors' GDPR obligations and demonstrating compliance, see Practice Notes, Data Processor Obligations Under the GDPR and Demonstrating Compliance with the GDPR: Accountability for Data Processors.

Controller Obligations

Hong Kong's Ordinance does not explicitly require data users to execute a written personal data processing agreement with processors. However, in practice, Hong Kong data users commonly enter into data processing agreements with processors and

the Commissioner strongly recommends their use in the non-mandatory guidelines on Outsourcing the Processing of Personal Data to Data Processors.

Controllers have specific obligations under the GDPR when engaging processors (Article 28, GDPR). The GDPR only permits transfers to processors when the processor sufficiently guarantees that it has implemented appropriate technical and organizational measures to protect personal data (Article 28(1), GDPR).

Processor relationships under the GDPR must be governed by a contract or other legal act under applicable law that binds the processor and that specifies:

- The subject matter and duration of the processing.
- The nature and purpose of the processing.
- The type of personal data processed.
- The categories of data subjects.
- The obligations and rights of the controller.

(Article 28(3), GDPR.)

Contracts with processors must also include certain terms specified in GDPR Article 28(3), which may differ from the terms recommended by the Commissioner. For example, unlike the Commissioner's guidance, the GDPR requires processors to:

- Implement measures to assist the controller in complying with data subjects' rights.
- Provide the controller with all necessary information for the controller to demonstrate compliance with the GDPR's obligations relating to engaging processors.

Hong Kong data users subject to the GDPR must comply with the GDPR's obligations applicable to engaging processors. Hong Kong entities audit any existing contracts to determine whether they contain the required contract terms and, if not, they should update existing contracts. For more on updating existing contracts, see Implementing the General Data Protection Regulation (GDPR) Checklist: Address Data Processor Requirements and Review and Update Vendor and Service Contracts.

Data Security

The Ordinance requires data users to take all practical steps to protect the personal data they hold against unauthorized or accidental access, processing, erasure, loss, or use (Principle 4, Ordinance). When developing measures to protect personal data, entities must consider:

- The type of personal data and the harm that may result from unauthorized or accidental access, processing, erasure, loss, or use.

- The physical location where they store personal data.
- Any security measures incorporated, by automated or other means, into any equipment that stores the personal data.
- Any measures it takes to ensure the integrity, prudence, and competence of persons accessing the personal data.
- Any measures it takes to ensure the secure transmission of personal data.

(Principle 4(1), Ordinance.)

Hong Kong entities subject to the Protection of Critical Infrastructures (Computer Systems) Bill (PCICS Bill), will need to consider implementing additional data security measures. The PCICS Bill will take effect on 1 January 2026. For more on information security under Hong Kong law, see Practice Note, Information Security Considerations (Hong Kong).

The GDPR requires controllers and processors to protect personal data by implementing appropriate technical and organizational measures to ensure a level of security appropriate to the risk (Article 32, GDPR). This includes implementing data protection by design and by default (Article 25, GDPR).

The GDPR highlights several appropriate security measures, including:

- Pseudonymization and encryption (see Practice Note, Anonymization and Pseudonymization Under the GDPR).
- Ensuring the ongoing confidentiality, integrity, availability, and resilience of data processing systems and services.
- Restoring availability and access to personal data in a timely manner if a physical or technical incident occurs.
- A process for regularly testing, assessing, and evaluating the effectiveness of the entity's technical and organizational security measures.

(Article 32(1), GDPR.)

When assessing the appropriate level of security, controllers and processors must consider the risks presented by the processing, including from accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of or access to personal data (Article 32(2), GDPR). A controller or processor may demonstrate compliance with GDPR Article 32 using an approved:

- Code of conduct.
- Certification mechanism.

(Articles 40 and 42, GDPR; see Certifications and Codes of Conduct.)

Hong Kong entities must audit their security practices to ensure compliance with the GDPR. For more on complying with the GDPR, see:

- Practice Note, Data Security Under the GDPR
- Implementing Data Security Measures Under the GDPR Checklist.
- Implementing the General Data Protection Regulation (GDPR) Checklist: Review Personal Data Protection and Security Measures and Data Protection by Design and Default.

Data Breach Notification

While the Ordinance does not require data subject or Commissioner notification of a data breach, the Commissioner recommends that data users notify regulators and individuals in certain circumstances and has issued Guidance on Data Breach Handling and the Giving of Breach Notifications. Hong Kong entities subject to the PCICS Bill, may also have regulator notification obligations. Entities are liable for fines for non-compliance. For more on data breach notification in Hong Kong, see Practice Note, Cyber Incident Response and Data Breach Notification (Hong Kong).

The GDPR establishes personal data breach notification requirements. A data breach under the GDPR means a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of or access to personal data (Article 4(12), GDPR). Controllers must notify:

- The relevant supervisory authority without undue delay and no later than 72 hours after any breach of personal data, unless the data breach is unlikely to pose a risk of harm (Article 33, GDPR).
- The data subject without undue delay if the personal data breach poses a high risk of harm, subject to certain limited exceptions (Article 34 and Recital 86, GDPR).

The GDPR requires processors to notify the controller without undue delay when they become aware of a data breach (Article 33(2), GDPR).

The EDPB has issued Guidelines on personal data breach notification under GDPR (EDPB 9/2022) (March 28, 2023) (GDPR Breach Guidelines I) and Guidelines on Examples regarding Personal Data Breach Notification (EDPB 01/2021) (December 14, 2021) (GDPR Breach Guidelines II) which each provide guidance on identifying data breaches, assessing risk of harm to data subjects, and providing notification to supervisory authorities and data subjects. GDPR Breach Guidelines II supplement GDPR Breach Guidelines I.

The GDPR only requires data subject notification when the security breach poses a high risk of harm to data subjects (Article 34(2), GDPR). Similar to the Commissioner's guidance, the GDPR requires controllers to assess the risk of harm to data subjects. Risks to data subjects may include, for example:

- Loss of control over personal data.
- Limitation of data subject rights.
- Discrimination.

- Identity theft or fraud.
- Financial loss.
- Damage to reputation.
- Significant economic or social disadvantage.

(GDPR Breach Guidelines I, at 9; GDPR Breach Guidance II, at 6 to 7.)

In certain situations, the controller is exempt from notifying data subjects (Article 34(3), GDPR; see GDPR Breach Guidelines I, at 22 and example cases in GDPR Breach Guidelines II).

Hong Kong entities subject to the GDPR must comply with the data breach notification requirements for EU personal data. Entities should conduct a gap analysis to compare their current incident response plans to the GDPR's requirements and develop plans to update relevant policies and procedures applicable to EU personal data. For more on complying with the GDPR's breach notification requirements, see:

- Practice Note, Data breach notification (UK).
- Implementing the General Data Protection Regulation (GDPR) Checklist: Follow Data Breach Notification Requirements.
- GDPR Breach Guidelines I.
- GDPR Breach Guidelines II.

Data Subject Rights

The GDPR provides more rights to data subjects than Hong Kong's Ordinance. The GDPR also:

- Requires controllers to help data subjects exercise their rights.
- Imposes several obligations on controllers when responding to data subject requests.

(Article 12(2), GDPR.)

Hong Kong controllers subject to the GDPR must understand their obligations when handling data subject requests and take steps to implement compliant response procedures for the different types of requests. For more on handling requests, see Handling Data Subject Requests Under the GDPR Toolkit.

This table compares data subject rights under the GDPR and the Ordinance. The sections below provide additional information on each data subject right.

Ordinance Data Subject Rights	GDPR Data Subject Rights
Information (Principle 1(3), Ordinance.)	Similar information right, but with broader content requirements (Articles 12 to 14 and Recitals 58 to 62, GDPR). To compare content requirements, see Notice.
Access their own personal data (Principle 6 and Section 18, Ordinance).	Access their own personal data (Articles 12 and 15 and Recital 63, GDPR). To compare requirements, see Access and Correction.
Correct personal data (Section 22, Ordinance).	Correct personal data (Article 16, GDPR). To compare requirements, see Access and Correction.
	Additional GDPR data subject rights not found in the Ordinance: • Erase personal data, also known as the right to be forgotten (Article 17 and Recitals 65 and 66, GDPR; see Erasure (Right to Be Forgotten)). • Object to data processing (Article 21 and Recitals 69 and 70, GDPR; see Processing Objection). • Restrict data processing (Article 18, GDPR; see Processing Restriction). • Receive a copy of their personal data or transfer their personal data to another controller (Article 20, and Recital 68, GDPR; see Right to Data Portability). • Not be subject to automated decision-making (Article 22 and Recital 71, GDPR; see Automated Decision-Making Objection). • Be notified of a data security breach (Article 34 and Recital 86, GDPR; see Data Security). Controllers must also notify third-party recipients of personal data about correction, erasure, and

	processing restriction requests and must inform the data subject about the recipients if the data subject requests this information (Article 19, GDPR). For more on these rights, see Practice Note, Data Subject Rights Under the GDPR.

Notice

The GDPR and the Ordinance both require entities to provide data subjects with a privacy notice that includes specific information about the entity's data collection and processing activities (Articles 13, 14, GDPR and Principle 1(3), Ordinance). Privacy notices under the Ordinance, also called personal information collection statements or PICSs, provide less information than privacy notices under the GDPR.

Ordinance Notice Requirements	GDPR Notice Requirements
Data users must provide the following information at or before the collection of the personal data: • Whether providing the data is mandatory or voluntary and the consequences for not supplying the personal data. • The purposes of use for the personal data. • The categories of recipients of the personal data. (Principle 1(3), Ordinance.) On or before the first use of the personal data, data users must provide the following information: • The data subjects' rights including access and correction. • The contact details of the person to which data subjects should send access and correction requests. (Principle 1(3), Ordinance.)	When a controller collects personal data directly from a data subject, it must first inform the data subject about: • The controller's identity and contact details and, if applicable, its EU representative's identity and contact details. • Contact details for the controller's data protection officer, if applicable. • The purposes for which the controller processes any personal data collected. • The legal basis for the processing. • Identification of the controller's legitimate interests when they serve as the legal basis for data processing. • The recipients or categories of recipients of the personal data, if any. • Whether the controller intends to transfer personal data outside of the European Economic Area (EEA) and the data transfer mechanism it uses to legalize the transfer.

For more, see Country Q&A, Data Protection in Hong Kong: Overview: Question 12 and Question 13.

- How long the controller stores the personal data or the criteria it uses to determine retention periods.
- Whether the data subject must provide the personal data by law, by contract, or for another reason and the consequences of not providing the personal data.
- Whether the controller uses automated decision-making, including profiling, the auto-decision logic used, and the consequences of this processing for the data subject.
- The data subject's rights including:
    - rights of access, rectification, erasure, restriction, objection, and data portability;
    - the right to withdraw consent and how to exercise that right; and
    - the right to make a complaint with a local supervisory authority and how to exercise that right, if applicable.

(Article 13, GDPR.)

When the controller obtains personal data about a data subject from a third party, the controller must also provide notice to the data subject. This notice must include the same information as the notice required when the controller collects personal data directly from a data subject. However, the controller:

- Must add to the notice:
    - the categories of personal data the controller collects; and
    - the source of the personal data, including whether it came from publicly accessible sources.

(Article 14, GDPR.)

	• Does not need to notify the data subject about whether the data subject must provide the personal data by law, by contract, or for another reason or the consequences of not providing the personal data. For more, see Practice Note, Data Subject Rights Under the GDPR: Information Right.

Privacy notices that comply with the Ordinance likely do not comply with the GDPR. Hong Kong controllers subject to the GDPR should:

- Audit existing privacy notices provided to EU data subjects and conduct a gap analysis to determine:
  - whether the existing notices meet the GDPR's requirements, including the transparency requirements (see Practice Note, Complying with the GDPR's Transparency Obligation to Data Subjects); and
  - what additional information the controller must provide to EU data subjects.
- Revise and issue new privacy notices to EU data subjects.

For more compliance steps, see Implementing the General Data Protection Regulation (GDPR) Checklist: Review and Update Privacy Notices and Updating Privacy Notices to Comply with the GDPR Checklist.

Access and Correction

Data subjects have similar access and correction rights under both the Ordinance and the GDPR. However, the Ordinance and the GDPR contain different procedural requirements for entities when responding to those requests.

Ordinance Access and Correction Rights	GDPR Access and Correction Rights
Data subjects have the right to: • Ascertain whether a data user holds their personal data. • Request access to their personal data, including receiving a copy. • Request correction of their personal data. (Principle 6 and Sections 18 and 22, Ordinance.)	Data subjects have the right to: • Obtain confirmation from the controller that it is processing their personal data. • Access their personal data, including receiving a copy on request unless providing a copy adversely affects the rights and freedoms of others. • Obtain certain information about the processing. • Correct inaccurate personal data.

For more information, see Country Q&A, Data Protection in Hong Kong: Overview: Question 12 and Question 13.	• Complete incomplete personal data. (Articles 15 and 16 and Recital 63, GDPR.) For more on the access and correction rights, see Practice Note, Data Subject Rights Under the GDPR: Personal Data Access Right and Personal Data Rectification Right.

For GDPR compliance steps, see Responding to Data Subject Requests Under the GDPR Checklist: Establish Steps for Responding to All Data Subject Requests, Provide Information, and Correct or Complete Personal Data.

Erasure (Right to Be Forgotten)

The Ordinance does not explicitly provide data subjects with an erasure right. However, the Ordinance requires data users to ensure that they do not retain personal data for any longer than necessary to fulfill the original collection purpose (or any directly related purpose) (Principle 2(2), Ordinance). Data users must erase personal data about Hong Kong data subjects once it is no longer necessary.

Under the GDPR, data subjects have the right to request the erasure of the personal data that a controller holds about them, also known as the "right to be forgotten" (Article 17 and Recital 65, GDPR). After a data subject requests erasure for one of the statutory reasons, the controller must erase it without delay unless an exception applies permitting retention.

For more on the erasure right, see Practice Note, Data Subject Rights Under the GDPR: Personal Data Erasure Right ("Right to Be Forgotten").

For steps to comply with the GDPR's erasure right, see Responding to Data Subject Requests Under the GDPR Checklist: Establish Steps for Responding to All Data Subject Requests and Erase Personal Data Unless Continued Retention is Necessary for Certain Purposes.

Processing Objection

The Ordinance does not explicitly give data subjects the right to object to data processing or the right to request that a data user stop processing their personal data. However, the Ordinance does require data users to provide notice and obtain consent before using personal data for direct marketing purposes and data subjects may refuse to consent for this purpose of use (Section 35C, Part 6A, Ordinance).

The GDPR provides data subjects with the right to object to data processing under certain circumstances (Article 21, GDPR). For more on when this right applies, see Practice Note, Data Subject Rights Under the GDPR: Data Processing Objection Right.

For steps to handle processing objections under the GDPR, see Responding to Data Subject Requests under the GDPR Checklist: Establish Steps for Responding to All Data Subject Requests and Stop Processing Personal Data.

Processing Restriction

The GDPR grants data subjects the right to restrict the processing of their personal data under certain circumstances (Article 18, GDPR). Hong Kong's Ordinance does not provide data subjects with a similar right. For more on when this right applies, see Practice Note, Data Subject Rights under the GDPR: Data Processing Restriction Right.

For steps to handle processing restriction requests, see Responding to Data Subject Requests Under the GDPR Checklist: Establish Steps for Responding to All Data Subject Requests and Review and Honor Processing Restriction Requests.

Right to Data Portability

The GDPR provides data subjects with a right to data portability. The data portability right grants individuals 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), (2) and Recital 68, GDPR.)

The Ordinance does not include a similar right. For more on when this right applies, see Practice Note, Data Subject Rights Under the GDPR: Data Portability Right.

For steps to handle data portability requests, see Responding to Data Subject Requests Under the GDPR Checklist: Establish Steps for Responding to All Data Subject Requests and Determine Whether the Data Portability Right Applies.

Automated Decision-Making Objection

Data subjects have similar automated decision-making rights under both the Ordinance and the GDPR. However, the GDPR provides data subjects with greater protection from a wider variety of data processing.

Ordinance Automated Data Processing	GDPR Automated Decision-Making
The Ordinance restricts the use of automated data processing that amounts to a "matching" procedure (Section 30, Ordinance). A matching procedure occurs when: • The data user compares two sets of personal data collected for different purposes using automated means. • Each comparison involves the personal data of ten or more data subjects.	Data subjects have the 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 (Article 22(1) and Recital 71, GDPR). This right does not apply when the automated decision is: • Necessary for entering into or performing a contract with the data subject.

- The purpose of the comparison is to:
  - verify the data; or
  - produce or verify data that the data user may use to take adverse action against any of the data subjects.

(Section 2, Part 1, Ordinance.)

A data user can only carry out a matching procedure if one of the following applies:

- The relevant data subject consents to the processing.
- The data user applies for and obtains Commissioner consent under Ordinance Sections 31 and 32.
- The Commissioner has given notice in the Gazette of a permitted class of matching procedures. To date, the Commissioner has not notified any permitted classes of matching procedures.

(Section 30, Ordinance.)

The Ordinance does not contemplate further uses or limitations on the use of automated data processing that does not amount to a matching procedure.

- Authorized by EU or member state law applicable to the controller if the law requires suitable measures to safeguard the data subject's rights, freedoms, and legitimate interests.
- Based on explicit data subject consent.

(Article 22(2), GDPR.)

The requirements for using automated data processing under the GDPR differ from restrictions on automated data processing that amounts to a matching procedure under the Ordinance.

When using automated decision-making that is necessary for entering into or performing a contract with the data subject or based on data subject consent, the controller must:

- Implement suitable measures to protect the data subject's rights.
- Allow the data subject to obtain human intervention for any automated decisions.
- Allow the data subject to express an opinion and contest any automated decisions.

(Article 22(3), GDPR.)

The controller must not use special categories of personal data in automated decision-making except under certain limited circumstances (Article 22(4), GDPR).

For more on using automated data processing under the GDPR and compliance steps for handling data subject objections, see Practice Notes:

- Data Subject Rights Under the GDPR: Automated Decision-Making Obligations.
- Profiling and Automated Decision-Making Under the GDPR.

- Responding to Data Subject Requests Under the GDPR Checklist: Establish Steps for Responding to All Data Subject Requests.
- Limit the Use of Solely Automated Decision-Making.

Cross-Border Data Transfers

GDPR Requirements

Controllers and processors transferring personal data outside of the EU must comply with certain requirements for data transfers established in Chapter V of the GDPR (Transfer of Personal Data to Third Countries or International Organisations). The GDPR provides several data transfer mechanisms for legally transferring personal data outside of the EU, including:

- An adequacy determination by the European Commission (Article 45, GDPR). The EU Commission has not deemed Hong Kong's Ordinance to provide adequate protection.
- Certifications and codes of conduct (see Certifications and Codes of Conduct).
- Where the controller or processor provides appropriate safeguards, if data subjects can enforce their legal rights and have effective legal remedies (Article 46, GDPR). Controllers and processors can provide appropriate safeguards without the approval of a supervisory authority by using:
    - a legally binding and enforceable instrument between public authorities or bodies;
    - binding corporate rules (Article 47, GDPR; see Practice Note, GDPR Controller BCR (EU));
    - standard data protection clauses adopted by the European Commission; or
    - standard data protection clauses adopted by a supervisory authority and approved by the European Commission.

  (Article 46(2), GDPR.)
- Appropriate safeguards with approval from a supervisory authority by using:
    - contractual clauses between the controller or processor and the controller, processor, or recipient in the non-EU country; or
    - provisions inserted into administrative arrangements between public authorities or bodies that include enforceable data subject rights.

  (Article 46(3), GDPR.)

Absent an adequacy decision or appropriate safeguards, GDPR Article 49 permits the cross-border transfer of personal data when the data subject explicitly consents. Valid consent under the GDPR is difficult to obtain, and entities should generally rely on another data transfer mechanism (see GDPR Consent Requirements).

GDPR Article 49 also permits the cross-border personal data transfers absent an adequacy decision or "appropriate safeguards" when the transfer is necessary for:

- Performing a contract.
- Important reasons of public interest.
- Establishing, exercising, or defending legal claims.
- Protecting the data subject's vital interests and the data subject is incapable of giving consent.
- Pursuing the controller's legitimate interests and the data subject's interests or rights and freedoms do not override those legitimate interests.

(Article 49(1), GDPR.)

For more information on cross-border data transfer mechanisms under the GDPR, see:

- Practice Note, Overview of EU General Data Protection Regulation: Cross-Border Data Transfers.
- GDPR Cross-Border Transfers Checklist.
- Data transfers toolkit (UK and EU).

Ordinance Requirements

Ordinance Section 33 restricts cross-border data transfers to help afford transferred personal data a level of protection comparable to that under the Ordinance. However, this section is not yet effective and there is no set date for implementation. The Commissioner has issued Guidance on Personal Data Protection in Cross-Border Data Transfer which includes guidance for complying with Section 33 when it takes effect.

Some data users may voluntarily adopt measures now to comply with Ordinance Section 33 and the Commissioner's guidance. Entities complying with Section 33 still need to take additional steps when transferring personal data outside of the EU to comply with the GDPR. For compliance steps, see Implementing the General Data Protection Checklist: Review Cross-Border Transfer Mechanisms.

For more on transferring personal data out of Hong Kong see, Practice Note, Cross-Border Personal Data Transfers (Hong Kong).

GDPR and Ordinance Statutory References

Subject Matter	GDPR Article	Ordinance Section
Extra-territorial application (see Extra-Territorial Application)	Article 3	N/A
EU representative (see EU Representative)	Article 27	N/A
Controller (data user) defined (see Controllers and Processors Defined)	Article 4(7)	Section 2
Processor defined (see Controllers and Processors Defined)	Article 4(8)	Principle 2(4)
Personal data defined (see Personal Data and Sensitive Personal Data Defined)	Article 4(1)	Section 2
Special categories of personal data (sensitive data) defined (see Personal Data and Sensitive Personal Data Defined)	Article 9	N/A
Data processing principles (see Principles Governing Personal Data Processing)	Article 5	Schedule 1
Data protection officers (see Compliance Measures Not Required by Hong Kong's Ordinance)	Article 37	N/A
Data protection by design and by default (see Compliance Measures Not Required by Hong Kong's Ordinance)	Article 25	N/A

Data protection impact assessments (see Compliance Measures Not Required by Hong Kong's Ordinance)	Article 35	N/A
Record of processing activities (see Compliance Measures Not Required by Hong Kong's Ordinance)	Article 30	N/A
Certifications and codes of conduct (see Certifications and Codes of Conduct)	Articles 40 and 42	N/A
Consent (see Conditions for Processing)	Articles 4(11) and 7(2)	Principle 3 and Section 35C(2)
Consent from minors (see Consent from Minors)	Article 8	N/A
Processor obligations (see Processor Obligations)	Articles 27, 28, 29, 30, 32, 33, 37, 44	N/A
Controller obligations when engaging processors (see Controller Obligations)	Article 28	Principles 2(3) and 4(2)
Data security (see Data Security)	Articles 25 and 32	Principle 4(1)
Data breach notification (see Data Breach Notification)	Articles 33 and 34	N/A
Data subject rights (see Data Subject Rights)	Articles 12 to 22 and 34	Principles 1(3), 2(2), and 6, and Sections 18, 22, 30, and 35C
Data subject information right (see Notice)	Articles 12 to 14	Principle 1(3)
Data subject access right (see Access and Correction)	Articles 12 and 15	Principle 6 and Section 18
Data subject correction right (see Access and Correction)	Article 16	Section 22

Data subject erasure right (see Erasure (Right to Be Forgotten))	Article 17	Principle 2(2)
Data subject processing objection right (see Processing Objection)	Article 21	Section 35C, Part 6A
Data subject processing restriction right (see Processing Restriction)	Article 18	N/A
Data subject data portability right (see Right to Data Portability)	Article 20	N/A
Data subject automated decision-making and automated data processing rights (see Automated Decision-Making Objection)	Article 22	Section 30
Cross-border data transfers (see Cross-Border Data Transfers)	Articles 44 to 50	Section 33

END OF DOCUMENT