European Union
General Data Protection Regulation
2016 (Effective 25 May 2018)
CONTENTS

Why is the GDPR relevant to Hong Kong organisations / businesses? 3
Extra-territorial application of the GDPR 4
Personal data covered by the GDPR 6
New Data Privacy Governance, Data Mapping and Impact Assessment 7
  a. Data Protection Officer 7
  b. Data Protection Impact Assessment 9
  c. Privacy by Design and by Default 10
  d. Data Mapping 11
Sensitive Personal Data 12
Consent 13
  a. Meaning of Consent 13
  b. Digital Consent for Minors 15
Mandatory Breach Notification 16
Data Processors' obligations 17
New and enhanced rights for individuals 20
  a. Enhanced right to notice on data processing 20
  b. Enhanced right to erasure ("right to be forgotten") 21
  c. Enhanced right to object to processing 23
  d. New right to restriction of processing 24
  e. New right to data portability 25
Data Protection Seals, Codes of Conduct and Cross-jurisdiction Data Transfer 26
  a. Certification / Seals and Codes of Conduct 26
  b. Cross-jurisdiction Data Transfer 27
Sanctions 28
More information on the GDPR 31
EU GDPR and HK PDPO (Major Differences) 32
This booklet aims at raising awareness amongst organisations / businesses in Hong Kong of the possible impact of the new regulatory framework for data protection in the European Union (EU) – General Data Protection Regulation 2016 (GDPR) and comparing some of the major requirements with those set out in the Personal Data (Privacy) Ordinance, Laws of Hong Kong (Cap 486) (PDPO).

The GDPR involves new provisions and enhanced rights. This booklet is, however, not intended to provide legal advice or interpretation in relation to the GDPR, nor is it meant to be a guide to compliance with the GDPR. The illustrations and examples in this booklet are direct quotes from the GDPR and the related guidance materials published by the European Commission. Organisations/businesses should seek specific legal advice to prepare themselves for the appropriate changes in their privacy policies, practices and procedures where appropriate.
The GDPR, adopted in 2016, will come into force on 25 May 2018.


In the wake of technological developments and globalisation, the constitutionalisation of the fundamental right to data protection in the EU and the fragmentation of legislature framework resulting from the EU Directive, the GDPR has the following main objectives and changes:

- harmonising and simplifying the framework for the digital single market;
- putting individuals in control of their data; and
- formulating a modern data protection governance.

\(^1\) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
Why is the GDPR relevant to Hong Kong organisations / businesses?

In Hong Kong, the PDPO was enacted to protect the privacy of individuals in relation to personal data. When the PDPO was drafted, reference was made to the relevant requirements under the OECD Privacy Guidelines 1980\(^2\) and the EU Directive. In consequence, the PDPO and the GDPR share a number of common features. Given that the GDPR constitutes significant developments, if not changes, of data protection law from the EU Directive, the new regulatory framework includes a number of requirements that are not found in the PDPO.

One of the key developments introduced under the GDPR to the data protection landscape outside the EU is the explicit requirement of compliance by organisations established in non-EU jurisdictions in specified circumstances. Given the diversified business or transaction models (e.g. online transactions), it is necessary for organisations / businesses in Hong Kong to ascertain if the GDPR is applicable to them, and hence be complied with.

---

\(^2\) The Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
Extra-territorial application of the GDPR

In a significant departure from the current requirements, an organisation / business in Hong Kong may need to comply with the GDPR if it:-

(1) has an establishment in the EU, where personal data is processed in the context of the activities of the establishment, regardless of whether the data is actually processed in the EU; or

(2) does not have an establishment in the EU, but offer goods or services to or monitor the behaviour of individuals in the EU.

An organisation / business is likely to be considered to have an EU "establishment" if it exercises "any real and effective activity", even a minimal one, through "stable arrangements" in the EU.

Examples of "establishments":

✓ Presence of sales offices, which promote, sell, advertise or market goods or services to individuals in the EU
✓ Appointment of sales agent or representative doing the above

The GDPR also applies to processing activities involving personal data engaged by organisations / businesses established in non-EU jurisdictions (including Hong Kong).

Generally, the GDPR may affect organisations / businesses established in the EU acting in the role of data controllers and data processors processing personal data in the context of that establishment, regardless of whether the personal data is actually processed in the EU.

---

3 Article 3 of the GDPR
4 See Weltimmo v. NAIH (C-230/14)
5 The term "data controller" in the GDPR is very similar in meaning to the term "data user" under the PDPO. Unlike the PDPO which does not regulate a data processor directly, the GDPR will impose on a data processor direct obligations on the protection of personal data privacy, the breach of which will attract administrative fines. More specific details will be provided in the subsequent paragraphs of this booklet.
6 See Article 29 Data Protection Working Party (WP29)'s EU General Data Protection Regulation: General Information Document
The GDPR attaches great weight to data processing. "Processing" is defined under Article 4(2) of the GDPR to mean "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction". The meaning of "processing" under the GDPR extends beyond the ordinary meaning of the word to include, amongst others, collection, recording, storage, adaptation, disclosure and erasure for the purposes of data processing.

The GDPR may also affect Hong Kong organisations / businesses without an establishment in the EU (either as data controller or data processor) if they process the personal data of individuals in the EU when offering goods or services or monitoring their behaviour.

Whether an organisation / business is offering goods or services to individuals in the EU may be ascertained where it is apparent that it intends to offer goods or services to individuals in one or more member states in the EU (irrespective of whether a payment is required). In this regard, the entirety of the circumstances will be taken into account.

Factors such as the use of a language or a currency of one or more member states in ordering goods and services, may make it apparent that the data controller envisages or targets at offering goods or services to individuals in the EU, and hence be caught by the GDPR.

Example: A Japanese web shop, offering products, available online in English with payments to be made in Euros, processing multiple orders a day from individuals within the EU and shipping these products to them.

(adopted from the Article 29 Data Protection Working Party (WP29)’s EU General Data Protection Regulation: General Information Document)
Personal data covered by the GDPR

The GDPR protects "personal data", which means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly".\(^7\)

The GDPR explicitly states that a range of identifiers can be personal data of a natural person such as name, identification number, location data, online identifier, or that the natural person is identifiable by reference to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Article 4(1)).

In determining whether a natural person is identifiable, the GDPR states that account should be taken of all the means reasonably likely to be used\(^8\).

---

\(^7\) Article 4(1) of the GDPR
\(^8\) Recital 26 of the GDPR
New Data Privacy Governance, Data Mapping and Impact Assessment

The GDPR expressly incorporates an accountability principle under Article 5(2). Organisations / businesses are required to (i) demonstrate their compliance with the principles of processing of personal data; (ii) implement appropriate technical and organisational measures to ensure compliance; and (iii) integrate data protection into their processing activities\(^9\).

When demonstrating compliance, organisations / businesses are required to take into account the nature, scope, context and purposes of processing, and the associated risks to the rights and freedoms of individuals.

More specifically, the measures or tools to demonstrate compliance and to implement or integrate data protection shall include:-

- appointment of a **Data Protection Officer (DPO)** to monitor, implement and advise on compliance with the GDPR\(^{10}\);
- undertaking **Data Protection Impact Assessment (DPIA)** to identify and manage data protection risks\(^{11}\);
- undertaking **Privacy by Design and by Default** to give effect to the data protection principles at the time of determining the means of processing and to integrate the necessary safeguards\(^{12}\);
- Keeping **records** of processing activities\(^{13}\); and
- drawing up data processing or handling **policies or practices** to demonstrate compliance and accountability\(^{14}\)

a. **Data Protection Officer**

A new significant measure to ensure compliance and accountability under the GDPR is the mandatory requirement for the appointment of a DPO. The DPO plays a key role in the data governance system and is tasked with the responsibility for implementing accountability tools (e.g. documentation for data processing activities and policies / procedures, DPIA). The EU **Guidelines on Data Protection Officers**\(^{15}\) provide guidance on the designation of a DPO, the expertise and skills required.

---

\(^9\) Articles 5, 24 and 25 of the GDPR
\(^{10}\) Article 37 of the GDPR (for the applicable types of organisations / businesses)
\(^{11}\) Article 35 of the GDPR
\(^{12}\) Article 25(1) of the GDPR
\(^{13}\) Article 30 of the GDPR
\(^{14}\) Article 24(2) of the GDPR
\(^{15}\) Issued by the WP29 and adopted on 5 April 2017 (http://ec.europa.eu/newsroom/document.cfm?doc_id=44100).
An organisation / business, regardless of its size, shall designate a DPO under any one of the following situations 16:

- it is a public authority or body (with minor exemptions for courts acting in a judicial capacity);
- its core activities 17 consist of processing operations which require regular and systematic monitoring 18 of data subjects on a large scale 19; or
- its core activities consist of processing a large scale of sensitive personal data and data relating to criminal convictions and offences.

In situations other than the above, the designation of a DPO will be on a voluntary basis.

The DPO shall perform at least the following tasks 20:

- to inform and advise the controller / processor and employees carrying out the processing of their obligations under the GDPR;
- to monitor compliance with the GDPR and data protection policies of the controller / processor, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- to provide advice where requested as regards the DPIA and monitor its performance; and
- to cooperate with the supervisory authority and act as contact point.

---

16 Article 37(1) of the GDPR
17 Generally, “core activities” can be considered as the key operations to achieve the data controller’s or processor’s objectives. These also include all activities where the processing of data forms an inextricable part of the controller’s or processor’s activities (see the EU Guidelines on Data Protection Officers).
18 Classic example of ”regular and systematic monitoring” will include activities such as online tracking, profiling, credit scoring, etc.
19 The GDPR does not define the meaning of “large scale”. It is not possible to give a precise number of the data subjects affected. However, the EU Guidelines on Data Protection Officers indicate that the following factors should be considered:-
    - the number of data subjects concerned;
    - the volume of data and/or the range of different data items being processed;
    - the duration, or permanence, of the data processing activity; and
    - the geographical extent of the processing activity.
20 Article 39(1) of the GDPR
It is crucial that the DPO is involved from the earliest stage possible in all issues relating to data protection, and participates regularly in meetings of senior and middle managements. His advice or presence is recommended when decisions with data protection implications are made, and his advice shall be given due weight. In this regard, organisations / businesses must provide sufficient resources for a DPO to carry out his task, and he should not be penalised or dismissed for performing his tasks\(^\text{21}\). The tasks and duties performed by a DPO must not put him in a conflict of interest situation, especially if he takes up senior management position or other duties involving the determination of purposes or means of processing of personal data\(^\text{22}\).

In Hong Kong, although the accountability principle and the related privacy management tools are currently not explicitly provided under the PDPO, the Privacy Commissioner for Personal Data (PCPD) encourages organisations / businesses to adopt the Privacy Management Programme\(^\text{23}\) (PMP) which manifests the accountability principle. The PMP serves as a strategic framework to assist an organisation / business in building a robust privacy infrastructure supported by an effective on-going review and monitoring process to facilitate compliance with the PDPO. It also demonstrates the organisation's / business' commitment to good corporate governance and building trust with its employees and customers through an open and transparent information policies and practices. The appointment of a data protection officer is recommended as a good practice under the PMP.

### b. Data Protection Impact Assessment

DPIA helps data controllers identify and manage data protection risks, avoid unnecessary costs (in terms of problems being discovered eventually), improve data security and avoid loss of trust and reputation.

\(^{21}\) See part 3 of the EU WP29 Guidelines on Data Protection Officers

\(^{22}\) Article 38(6) of the GDPR

Pursuant to the GDPR, a data controller is required to conduct DPIA prior to engaging in any processing which is likely to result in high risks to the rights and freedoms of individuals by virtue of the nature, scope, context and purposes of the data processing of the data controller\textsuperscript{24}. In particular, DPIA is required when it involves\textsuperscript{25}:-

- a systematic and extensive evaluation of individuals' personal aspects based on automated processing, including profiling, and on which decisions are made producing legal effects on or significantly affecting individuals;
- large-scale processing of sensitive personal data or data relating to criminal convictions or offences; or
- a systematic monitoring of a publicly accessible area on a large scale.

The PCPD has published an \textit{Information Leaflet on Privacy Impact Assessments}\textsuperscript{26} to guide organisations / businesses in Hong Kong in conducting their own assessments on activities which may have serious impacts or risks on privacy protection in relation to personal data. The PCPD also advises data users (or controllers) to carry out privacy impact assessment, for example, before using CCTV covering public places or common areas of buildings\textsuperscript{27}.

\section*{Privacy by Design and by Default}

Organisations / businesses are required to implement appropriate technical and organisational measures (such as pseudonymisation and data minimisation) which are designed to give effect to the data protection principles at the time of determining the processing activities, and to integrate the necessary safeguards with the processing in order to meet the requirements of the GDPR\textsuperscript{28}.

For data protection by design, consideration may be given to the following factors:-

- nature, scope, context and purposes of processing;
- risks level for the rights and freedoms of individuals;

\begin{itemize}
\item \textsuperscript{24} See WP29 Guidelines on Data Protection Impact Assessment
\item \textsuperscript{25} Article 35 of the GDPR
\item \textsuperscript{26} See PCPD’s website: www.pcpd.org.hk/english/resources_centre/publications/files/InfoLeaflet_PIA_ENG_web.pdf
\item \textsuperscript{27} See Guidance on CCTV Surveillance and Use of Drones issued by the PCPD, available at www.pcpd.org.hk/english/resources_centre/publications/files/GN_CCTV_Drones_e.pdf
\item \textsuperscript{28} Article 25(1) of the GDPR
\end{itemize}
the technological development; and
- cost of implementation.

In addition, appropriate technical and organisational measures are required to ensure, by default, that only personal data which is necessary for each specific purpose is processed. This requirement applies to the amount of data collected, the extent of processing, the storage period and the data accessibility.

### d. Data Mapping

Organisations / businesses (both in the capacity of a data controller or processor) are required to keep record of their processing activities, including the types of data processed, the purposes for which the data is used, the transfer of personal data to a third country or an international organisation / business etc.

Organisations / businesses that employ fewer than 250 people will be exempted unless (i) the processing they carry out is likely to result in a risk to the rights and freedoms of data subjects, (ii) their core activities involve processing sensitive personal data, personal data relating to criminal convictions and offences or large scale systematic monitoring activities.

Organisations / businesses may design templates to stocktake and categorise the various types of their processing activities. In designing the suitable templates, it is advisable to use simple language in concise terms but with some details for explanation. The record must be kept under regular review to ensure up-to-date, which is the key step to assist the DPO or the organisation / business in assessing the next steps required for achieving data protection governance.

Organisations / businesses should also draw up the appropriate policies and practices in relation to personal data protection for their staff to follow.

Although record keeping is not explicitly stated as a requirement under the PDPO, organisations / businesses in Hong Kong are required to make their privacy policies and practices transparent.

---

29 Article 25(2) of the GDPR
30 For other details of the record, see Article 30(1) and (2) of the GDPR
31 Article 30(5) of the GDPR
32 Data Protection Principle (DPP) 5 in Schedule 1 of the PDPO
Sensitive Personal Data

The GDPR imposes more stringent requirements than the existing EU Directive on the processing of special categories of personal data. These categories of personal data are considered inherently sensitive in view of their intrinsic and immutable nature, or the likelihood of serious harm or discriminatory consequences that may be inflicted on the individuals in case of mishandling.

Under the GDPR, the "special categories" of personal data refer to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or data concerning a natural person’s sex life or sexual orientation, and genetic data or biometric data processed for the purpose of uniquely identifying a natural person. (new items (underlined) added as compared with the EU Directive)

The GDPR imposes a general prohibition against the processing of these special categories of personal data unless one of the specified conditions is satisfied. The conditions include (i) the data subjects have given explicit consent to the processing; or (ii) where the processing is necessary for reasons of substantial public interest, which is proportionate to the aim pursued, etc.

In Hong Kong, the PDPO does not provide more stringent requirements for categories of personal data that are considered sensitive. It must however be noted that the PDPO requires organisations / businesses to take into account the type of personal data when considering the appropriate measures to be implemented to ensure the security of the data.

---

33 Article 9 of the GDPR  
34 For other conditions governing sensitive personal data, please refer to Article 9(2) of the GDPR  
35 See DPP4 in Schedule 1 to the PDPO
Consent

Under the GDPR, "consent" of the data subject is one of the legal bases for lawful processing of personal data.

In brief, the bases for lawful processing of personal data under the GDPR include:

- consent of the data subject to the processing for one or more specific purposes; or
- performance of a contract with the data subject or to take steps preparatory to such a contract;
- compliance with a legal obligation;
- protecting the vital interests of a data subject or another person where the data subject is incapable of giving consent;
- performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;
- purposes of legitimate interests.

a. Meaning of Consent

The GDPR defines "consent" as a freely given, specific, informed, and unambiguous indication of a data subject signifying his agreement to processing of personal data by either a statement or a clear affirmative action. (emphasis added)
When obtaining consent from data subjects in the form of a written declaration, organisations / businesses are required to present with a request for consent separately from other matters in an intelligible and easily accessible form using clear and plain language\textsuperscript{38}. Data subjects should also be informed of their right to withdraw their consent.

\begin{itemize}
  \item \textbf{Examples of valid and invalid consent:}
    \begin{itemize}
      \item \textbf{X} An individual is not allowed to give separate consent for different personal data processing operation
      \item \textbf{X} Bundled consent situation where the performance of a service contract is made conditional on the consent given to such processing activities which are unnecessary
      \item \textbf{X} Default setting to pre-tick a box to agree on the terms and conditions
      \item \textbf{X} Silence and inaction of the data subject
      \item \textbf{✓} Ticking a box when visiting a website for its terms and conditions
      \item \textbf{✓} Choosing the technical settings for an app installed for smartphone
    \end{itemize}
\end{itemize}

\textsuperscript{38} Article 7 of the GDPR
b. **Digital Consent for Minors**

Organisations / businesses must give special attention when seeking children’s consent in relation to the processing of their personal data for the provision of "information society services"\(^{39}\) (e.g. e-commerce businesses, online marketplaces offering of online information, internet referencing services offered by search engines, etc.). Under the GDPR, for children who are below 16 years old (or 13 years old in some of the EU member states), their consent must be given or authorised by a person with parental responsibility\(^{40}\).

In Hong Kong, despite the fact that the PDPO does not explicitly require consent as one of the bases for collection of personal data, organisations / businesses are required to provide notification to individuals on the purposes of collection, and obtain their "prescribed consent" if they use the personal data for a purpose not directly related to the original collection purpose. "Prescribed consent" is defined to mean an express consent given voluntarily which has not been withdrawn by notice in writing. The PCPD’s regulatory stance is that the consent must be informed, and cannot be inferred from inaction and silence. Similarly, the PCPD has stressed that it would be good practice for organisations / businesses to provide individuals with an option to consent in circumstances not bundled with other terms or conditions unnecessary for their provision of services.

In respect of a vulnerable individual data subject who is a (i) minor\(^{41}\), (ii) incapable of managing his own affairs, or (iii) mentally incapacitated, the PDPO does not specifically provide for digital consent but allows the "relevant person"\(^{42}\) to give prescribed consent on his behalf, if the relevant person has reasonable grounds to believe that the use of the data for the new purpose is clearly in the interest of the data subject\(^{43}\).

---

39 Pursuant to Article 1(1)(b) of Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015, “information society services” is defined as “any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.”

40 Article 8 of the GDPR

41 In the absence of specific definition under the PDPO, a “minor” refers to an individual who is below 18 years old (See section 3, Interpretation and General Clauses Ordinance (Cap 1), Laws of Hong Kong SAR. A person shall reach majority at the age of 18 under the Age of Majority (Related Provisions) Ordinance (Cap 410)).

42 “Relevant person” includes (i) the minor’s parent; (ii) a person appointed by a court to manage his affairs or (iii) the guardian of the mentally incapacitated individual (section 2(1) of the PDPO).

43 DPP3(2) in Schedule 1 to the PDPO
Mandatory Breach Notification

Under the GDPR\(^{44}\), it is mandatory for organisations / businesses to give data breach notification. They are required under the GDPR to advise the supervisory authority in the EU member states of a data breach without undue delay (and where feasible, no later than 72 hours after becoming aware of it) unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. Notification to the affected individuals is required if the data breach is likely to result in a "high risk to the rights and freedoms" of individuals unless under exempted circumstances\(^ {45}\). The same obligation is imposed on organisations / businesses which are acting in the role of data processors.

The prescribed contents to be included in a data breach notification to the supervisory authority\(^ {46}\):

- nature and likely consequences of the breach;
- categories and approximate number of data subjects and personal data concerned;
- measures taken or intends to be taken to mitigate any adverse effects of the breach; and
- contact details of DPO of the organisation / business or other contact point.

Breach notification in Hong Kong is on a voluntary basis. The PCPD has published the Guidance on Data Breach Handling and the Giving of Breach Notifications\(^ {47}\), which explains the steps to be taken for giving notification. It is a recommended good practice for organisations / businesses to give notification to the PCPD and any affected individuals as soon as possible so as to ensure that steps will be taken without undue delay to mitigate any possible harm.

---

\(^{44}\) Article 33

\(^{45}\) Under Article 34(3) of the GDPR, no reporting to the affected data subjects is required where:-
(a) appropriate technical and organisational protection measures were in place, in particular those that render the data unintelligible to unauthorised parties (e.g. encryption);
(b) data controller has taken subsequent measures which ensure that the anticipated high risk to the rights and freedoms of data subjects is no longer likely to materialise; or
(c) it would involve disproportionate effort, in which case a public communication to inform the data subjects would be an alternative.

\(^{46}\) Articles 33-34 and Recitals 85-86 of the GDPR

Data Processors' obligations

Organisations / businesses in Hong Kong taking up the role as data processors (e.g. service providers engaged by EU established enterprises to analyse personal data, cloud service providers, etc. solely for the purposes directed by the enterprises) may be affected by the new and extensive requirements under the GDPR.

Firstly, the GDPR requires a data controller to appoint or choose only data processors that provide sufficient guarantees in respect of technical measures and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subjects. In addition, contractual or legal act shall be adopted by the data controller to bind the processors in this respect. The GDPR provides specific clauses that must be included in such contracts to:

- process personal data only on the controller's documented instructions;
- ensure that persons authorised to process personal data are committed to confidentiality or are under an appropriate statutory obligation of confidentiality;
- ensure security of personal data it processes;
- follow specified conditions in engaging another processor;
- assist the controller to respond to requests for exercising the data subject's rights in GDPR (e.g. Chapter III - data access rights, rights to rectification, etc.);
- assist the controller to comply with obligations of data security and DPIA;
- at the choice of the controller, delete or return all personal data to the controller after the end of processing, and delete existing copies unless the law requires storage of the data; and
- provide the controller with information necessary to demonstrate compliance with the obligations, and allow for and contribute to audits, including inspections, to be conducted by the controller.

48 Article 28 of the GDPR
49 Article 28(3) of the GDPR
The GDPR also imposes direct obligations on data processors including (but not limited to)\(^50\):

- not to engage another processor without the controller’s authorisation;
- maintain records of processing activities;
- cooperate with supervisory authority on request in the performance of its tasks;
- process under the controller’s instructions unless required by law;
- ensure security of processing;
- report data breach to controllers without undue delay;
- designate a DPO; and
- transfer personal data outside EU under prescribed conditions only.

The GDPR includes a limited exception for organisations with fewer than 250 employees with regard to record-keeping. In addition, the supervisory authorities in the EU are encouraged to take account of the specific needs of micro, small and medium-sized enterprises\(^51\) in the application of the GDPR.

Data Processors are regulated directly by data protection authorities under the GDPR, and they are liable to be penalised for breach of their obligations (e.g. failure to report a data breach)\(^52\).

\(^{50}\) For the respective direct obligations on data processors, see Article 28(2); Recital 82, Article 30(2) and 30(4); Article 31; Article 29; Article 32(1); Article 33(2); Article 37(1) and Articles 45-47 and 49 of the GDPR.

\(^{51}\) Article 2 of the Annex to Commission Recommendation 2003/361/EC states:

1. The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million.

2. Within the SME category, a small enterprise is defined as an enterprise which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million.

3. Within the SME category, a microenterprise is defined as an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million.

\(^{52}\) Articles 58, 77, 79, 82 and 83 of the GDPR
Organisations / businesses acting merely as data processors\textsuperscript{53} in Hong Kong are not directly regulated under the PDPO\textsuperscript{54}. They are however made subject to indirect obligations in that their principals being data users are required to adopt contractual or other means to (i) prevent data transferred to data processors from being kept longer than is necessary for processing, and (ii) prevent unauthorised or accidental access, processing, erasure, loss or use of the data\textsuperscript{55}. Their principals will be held accountable for the infringing acts or practices performed on their behalf with express or implied authority\textsuperscript{56}. With regard to data protection on outsourcing activities, the PCPD has published the \textit{Information Leaflet: Outsourcing the Processing of Personal Data to Data Processors} to assist organisations with the recommended contractual and non-contractual measures\textsuperscript{57}.

\textsuperscript{53} Data processor means a person who: (a) processes personal data on behalf of another person; and (b) does not process the data for any of his own purposes (DPP2(4) of the PDPO).

\textsuperscript{54} Under section 2(12) of the PDPO, a person is not a data user in relation to any personal data which the person holds, processes or uses solely on behalf of another person if, but only if, that first-mentioned person does not hold, process or use, as the case may be, the data for any of his own purposes.

\textsuperscript{55} Pursuant to DPP2(3) and 4(2) in Schedule 1 to the PDPO

\textsuperscript{56} Section 65(2) of the PDPO

\textsuperscript{57} See PCPD’s website: www.pcpd.org.hk/english/resources_centre/publications/files/dataprocessors_e.pdf
**New and enhanced rights for individuals**

The GDPR maintains, reinforces and further enhances the rights of individuals in various aspects (on information, access, rectification, objection, restriction, erasure, right to be forgotten and right to data portability).

**a. Enhanced right to notice on data processing**

The GDPR requires organisations / businesses to give individuals a range of prescribed information about the processing of their personal data subject to certain exceptions\(^{58}\). The prescribed information must be presented in a concise, transparent, intelligible and easily accessible manner. Hence, organisations / businesses should review their personal information collection statement or privacy policies and practices for compliance with an individual’s enhanced right to notice under the GDPR.

Generally, the prescribed information includes\(^{59}\):

- data controller's identity and contact details, contact details of DPO (if appointed)
- purpose and basis for processing (e.g. legitimate interest to process the data)
- right to withdraw consent (if processing is based on consent) and the right to object to such processing
- categories of recipients of data
- retention period
- right to erasure
- existence of automated decision making about the individual and the logic behind
- right to complain to the relevant data protection authority
- whether provision of data is mandatory and the consequence of non-provision
- information on cross-jurisdiction data transfers
- source of data (if not collected from the individual)

---

\(^{58}\) Under Article 14(5) of the GDPR, the exceptions can be summarised as (1) the data subject already has the information; (2) disproportionate effort; (3) disclosure as permitted by law and measures are taken to protect data subject’s legitimate interests; and (4) secrecy obligation.

\(^{59}\) Articles 13 and 14 of the GDPR
In Hong Kong, while organisations / businesses are required to notify the individuals about certain items of information when collecting personal data directly from them, and they must be transparent in their privacy policy and practices in this regard\(^{60}\), the PDPO is less extensive in terms of the items of prescribed information to be notified to the individuals for data processing purposes. The GDPR explicitly requires notification to be given for data processing purposes even though the personal data is not collected directly from the individuals, unless under limited exceptions\(^{61}\).

Organisations / businesses in Hong Kong are encouraged to be transparent in their data handling practices. The PDPO contains a proviso (i.e. under DPP1(3) in Schedule 1 to the PDPO) to exempt the notification requirement upon collection if so doing will be likely to prejudice the exempted purposes under Part 8 of the PDPO\(^{62}\).

**b. Enhanced right to erasure ("right to be forgotten")**

The right to erasure (also known as the "right to be forgotten")\(^{63}\) under the GDPR gives an individual a right to require organisations / businesses to delete his personal data without undue delay under specified circumstances, including (i) where the personal data is no longer necessary in relation to the purposes for which it is collected, (ii) where the individual withdraws the consent (which forms the basis of processing), (iii) where there is no overriding legitimate interest, or (iv) the personal data collected is about children in relation to an information society service, etc.

---

\(^{60}\) See DPP1(3) and 5 in Schedule 1 to the PDPO  
\(^{61}\) Article 14 of the GDPR  
\(^{62}\) Part 8 of the PDPO provides specific exemptions to the application of the DPPs, including collection, use and access  
\(^{63}\) Article 17 of the GDPR
A data controller who has made public disclosure of personal data (e.g. disclosure on the Internet) has to take reasonable steps (taking account of available technology and implementation cost) to inform the other controllers (e.g. a search engine) which are processing the data about a data subject's request for erasure of any links to or copy of the data\textsuperscript{64}.

The GDPR explicitly recognises certain exceptions where retention of the data is necessary:-

- for exercising the right of freedom of expression and information;
- for compliance with a legal obligation, or performance of a task carried out in the public interest or in the exercise of official authority;
- for reasons of public interest (e.g. in the area of public health, management of health or social care systems and services, etc.);
- for archiving, scientific or historical research purposes or statistical purposes in the public interest; or
- for the establishment, exercise or defence of legal claims\textsuperscript{65}.

In Hong Kong, the requirements concerning erasure can be found in DPP2(2) in Schedule 1 to the PDPO and section 26. Generally, a data user is imposed with an obligation to take all practicable steps to erase personal data that is no longer necessary for the original collection purpose (including any directly related purpose). Section 26 of the PDPO provides exceptions to such obligation where the erasure is prohibited by law or it is against the public interest to erase the data.

\textsuperscript{64} Article 17(2) of the GDPR
\textsuperscript{65} Article 17(3) of the GDPR
c. Enhanced right to object to processing

The GDPR provides the right to object at any time to the processing including profiling, of one’s personal data which is based on the following grounds:

(a) the performance of a task carried out in the public interest or in the exercise of an official authority vested in the data controller;
(b) the legitimate interests pursued by the data controller or third party;
(c) direct marketing purposes; or
(d) scientific or historical research purposes or statistical purposes.

"Profiling" is defined under Article 4(4) of the GDPR, as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".

Examples of profiling:

- Figuring out a person's preferences, hobbies and habits by analysing his Internet browsing and purchase histories
- Analyses or predictions concerning an individual's credit applications without human intervention

Upon receipt of the objection to the processing activities which are based on the above grounds (a) and (b), the data controller must cease the processing of the personal data (including profiling) unless it can demonstrate compelling legitimacy grounds which override the individual's interests, rights and freedom, or for the establishment, exercise or defence of legal claims in order to maintain the processing of personal data (including profiling).
In relation to processing personal data for the above ground (d) (i.e. scientific or historical research purposes or statistical purposes), an individual may object by relying on his or her particular situation unless the processing is necessary for the performance of a task carried out in the public interest\textsuperscript{68}. However, no exception shall apply to processing of personal data purely for direct marketing purpose\textsuperscript{69}.

Under the PDPO, an individual in Hong Kong is not generally given the right to request an organisation / business to stop "processing”\textsuperscript{70} his personal data. Nevertheless, they are required to provide notification to and obtain consent from an individual before using his personal data for direct marketing purpose. In addition, an individual is given the right to opt-out from the use or provision for use of his personal data in direct marketing under Part 6A of the PDPO.

d. New right to restriction of processing

Under the GDPR, in the circumstances mentioned below, an individual is given the right to restriction of processing of his personal data from a data controller who may then store the data only for an interim period\textsuperscript{71} if:

- an individual contests the accuracy of his personal data, the data controller is required to restrict processing for a period of time enabling the controller to verify the accuracy;
- the processing is unlawful and the individual opposes the erasure of the personal data and requests restriction on the use instead;
- the personal data is no longer needed for the processing, but required by the individual for the establishment, exercise or defence of legal claims; and
- the individual has objected to the processing of the personal data pending verification as to whether the legitimacy grounds of the controller can override those of the individual.

\textsuperscript{68} Article 21(6) of the GDPR  
\textsuperscript{69} Article 21(2) of the GDPR  
\textsuperscript{70} Under Articles 6(1)(a), 4(2), 4(11), 7, 8, Recital 43 and 32 of the GDPR, "processing" covers a wide meaning ranging from collection, use, disclosure, storage, combination to erasure of personal data depending on the context, see also preceding paragraphs on "Extraterritorial application of the GDPR".  
\textsuperscript{71} Article 18 of the GDPR
In response to a data correction request, an organisation / business in Hong Kong is required under the PDPO to take reasonably practicable steps to notify the third party to whom the inaccurate data has been supplied during the last 12 months if there is no reason to believe the third party has ceased to so use the data\(^\text{72}\).

### e. New right to data portability

This new right entitles an individual to obtain from a data controller, and to transmit to another data controller, a copy of his personal data in a structured, commonly-used and machine-readable format, where:

- the legal basis of processing is either the individual's consent or the performance of a contract; and
- the processing is carried out by automated means\(^\text{73}\).

This right is confined to personal data which has been provided by the individual to the data controller. As explained in the *Guidelines on the Right to Data Portability*\(^\text{74}\), this new right facilitates individuals' ability to move, copy or transmit their personal data held by one data controller to another. That said, the two controllers are not obliged to make their technically incompatible systems compatible\(^\text{75}\).

The PDPO in Hong Kong does not provide equivalent right to restrict processing of personal data or right to data portability. Nonetheless, organisations / businesses are required to comply with data access and correction requests from individuals for their personal data\(^\text{76}\).

---

\(^{72}\) DPP2(1)(b)(i) of the PDPO  
\(^{73}\) Article 20 of the GDPR  
\(^{74}\) Issued by the EU WP29 in December 2016  
\(^{75}\) Recital 68 of the GDPR  
\(^{76}\) DPP6 in Schedule 1 and Part 5 of the PDPO
Data Protection Seals, Codes of Conduct and Cross-jurisdiction Data Transfer

a. Certification / Seals and Codes of Conduct

The GDPR explicitly recognises privacy seals or marks to demonstrate compliance. The regulatory authorities, the European Data Protection Board (which replaces the WP29) and the European Commission shall encourage the establishment of data protection certification mechanisms for the purpose of demonstrating compliance by controllers and processors. Certification may be relevant to organisations / businesses engaging in cloud computing or multi-layer of processing where individual audits or customised contractual clauses for data protection may not be feasible.

Certification may be issued for a maximum period of three years subject to renewal or withdrawal where the conditions or requirements are no longer met. It can be issued by either private or public accredited certification bodies, subject to the criteria developed by the data protection authority, or the European Data Protection Board, pursuant to the GDPR. Where the criteria are approved by the Board, it may result in a common certification, the European Data Protection Seal.

Certification is on a voluntary basis. The information relating to the certification will be made transparent and the certification marks will be maintained in a publicly available register.

Another aspect is that the GDPR encourages the drawing up of sector specific codes of conduct by associations and other bodies for application of the GDPR taking into account of the features of various processing sectors, and the needs of micro, small and medium-sized enterprises. The supervisory authorities in the member states within the EU shall approve or give comments on whether the code of conduct submitted complies with the GDPR. In this regard, Part 3 of the PDPO also provides for the approval of codes of practice by the Privacy Commissioner of Hong Kong after consultation with the relevant bodies representative of data users and interested parties.

77 Article 42(1) of the GDPR
78 Article 42(7) of the GDPR
79 Article 42(5) of the GDPR
80 Article 40 of the GDPR
81 Section 12 of the PDPO
b. Cross-jurisdiction Data Transfer

Transfer of personal data to third countries or international organisations outside the EU continues to be regulated under the GDPR\textsuperscript{82}. Personal data may be transferred to countries or international organisations outside the EU that provide an adequate level of data protection. The current requirements under the EU Directive are largely preserved in this regard.

Furthermore, adherence to the safeguards under such a certification mechanism or an approved code of conduct, combined with binding and enforceable commitments by the controllers / processors in the third country to apply those appropriate safeguards, could constitute one of the bases for cross-jurisdiction transfer of personal data to jurisdictions outside the EU\textsuperscript{83}.

The GDPR also provides detailed criteria that will be considered when determining whether a non-EU country or international organisation ensures adequate level of protection to the personal data transferred\textsuperscript{84}. The European Data Protection Board is required to provide the European Commission with an opinion assessing the adequacy of a country or international organisation’s level of protection\textsuperscript{85}.

In the absence of an adequacy decision\textsuperscript{86} made by the European Commission, the mechanisms or safeguards (apart from certification mechanism) that may be relied on for international transfer will include adopting standard contractual clauses and binding corporate rules approved by the EU\textsuperscript{87}.

The PDPO does not, however, expressly refer to certification mechanism or privacy seals / marks.

\textsuperscript{82} Chapter V of the GDPR
\textsuperscript{83} Articles 46 (2)(e) & (f) and 42(5) of the GDPR
\textsuperscript{84} Article 45 of the GDPR
\textsuperscript{85} Article 45(2) of the GDPR
\textsuperscript{86} An adequacy decision refers to a decision of the European Commission that a third country, territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection (Article 45(1) of the GDPR).
\textsuperscript{87} Articles 46 and 47 of the GDPR
Sanctions

Article 58(2)(i) of the GDPR empowers supervisory authorities in the EU to impose two-tier administrative fines on data controllers and data processors for contravention of the GDPR.

Pursuant to Article 83(4) of the GDPR, a lower tier of administrative fine (i.e. up to €10 million, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of preceding financial year, whichever is higher) shall be imposed for failure to comply with the following requirements (non-exhaustive)\(^{88}\):

1. obtaining parental consent for processing of children’s personal data;
2. processing personal data anonymously if it is not necessary to identify the data subjects;
3. giving data breach notification;
4. conducting data protection impact assessment; and
5. appointing data protection officer.

Pursuant to Article 83(5) of the GDPR, an upper tier of administrative fine (i.e. up to €20 million, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of preceding financial year, whichever is higher) shall be imposed for failure to satisfy the following requirements (non-exhaustive)\(^{89}\):

1. complying with the basic principles for processing, such as lawful and fair processing or processing based on consent;
2. complying with data subjects’ rights, such as right to notice, right of access to personal data, right to rectification of personal data, right to erasure (right to be forgotten), right to object to processing, right to object to automated decision making, including profiling; and
3. transferring personal data to a recipient in a third country or international organisation pursuant to the lawful mechanisms.

---

\(^{88}\) See Article 8; Article 11; Article 33; Article 35 and Article 37 of the GDPR

\(^{89}\) See Articles 5-6; Articles 13-22 and Articles 44-49 of the GDPR
In Hong Kong, if an organisation / business fails to comply with a requirement under the PDPO (including the DPPs in Schedule 1), the Privacy Commissioner may issue an Enforcement Notice, directing it to remedy and, if appropriate, prevent any recurrence of the contravention pursuant to section 50 of the PDPO. Non-compliance with the Enforcement Notice is an offence. Criminal offences are also created to deal with the more serious infringements for contravention of other requirements, for example, direct marketing activities under Part 6A of the PDPO. Penalties for criminal offences are determined by courts in Hong Kong and the Privacy Commissioner has no power to impose administrative fines.
The European Data Protection Board will have the legal status of an EU body to settle disputes amongst data protection authorities of member states, and issue opinions, guidelines, recommendations and best practices.

For more information, organisations / businesses may refer to the website of the European Commission on Protection of Personal Data for details and the related guidance materials. (http://ec.europa.eu/justice/data-protection/index_en.htm)

A specific webpage on the GDPR, with regular updates, can also be found on PCPD's website (www.pcpd.org.hk)
## EU GDPR and HK PDPO (Major Differences)

<table>
<thead>
<tr>
<th>Application</th>
<th><strong>EU</strong></th>
<th><strong>HK</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Data processors or controllers:</td>
<td>• with an establishment in the EU, or</td>
<td>Data users (controllers / processors) who, either alone or jointly or in common with other persons, control the collection, holding, processing or use of the personal data in or from Hong Kong. [s.2(1)]</td>
</tr>
<tr>
<td>• established outside the EU, that offer goods or services to, or monitor the behaviour of individuals in the EU. [Art 3]</td>
<td><strong>Personal Data</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>&quot;Personal data&quot; means</th>
<th>&quot;Personal data&quot; means any data –</th>
</tr>
</thead>
<tbody>
<tr>
<td>• any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly.</td>
<td>• relating directly or indirectly to a living individual;</td>
</tr>
<tr>
<td>• examples of personal data explicitly identified being extended to include location data and online identifier. [Art 4(1)]</td>
<td>• from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and</td>
</tr>
<tr>
<td></td>
<td>• in a form in which access to or processing of the data is practicable. [s.2(1)]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Accountability and Governance</th>
<th>Risk-based approach; data controllers are required to:</th>
<th>The accountability principle and the related privacy management measures are not explicitly stated.</th>
</tr>
</thead>
<tbody>
<tr>
<td>• implement technical and organisational measures to ensure compliance [Art 24];</td>
<td>The Privacy Commissioner advocates the adoption of a privacy management programme which manifests the accountability principle. The appointment of data protection officers and the conduct of privacy impact assessment are recommended good practices for achieving accountability.</td>
<td></td>
</tr>
<tr>
<td>• adopt data protection by design and by default [Art 25];</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• conduct data protection impact assessment for high-risk processing [Art 35]; and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• (for certain types of organisations) designate Data Protection Officers. [Art 37]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| Sensitive Personal Data | Category of sensitive personal data expanded. Processing of sensitive personal data is allowed only under specific circumstances. [Art 9] | No distinction between sensitive and non-sensitive personal data for all purposes. |</p>
<table>
<thead>
<tr>
<th><strong>Consent</strong></th>
<th><strong>EU</strong></th>
<th><strong>HK</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Consent must be</td>
<td>• freely given, specific and informed;</td>
<td>Consent is not a pre-requisite for the collection of personal data, unless the personal data is used for a new purpose. [DPP1&amp;3] For other purposes, where consent is also required, consent means express and voluntary consent.</td>
</tr>
<tr>
<td></td>
<td>• an unambiguous indication of a data subject’s wishes, by statement or by clear affirmative action, which signifies agreement [Art 4(1)]; and</td>
<td>No requirement for parental consent.</td>
</tr>
<tr>
<td></td>
<td>• given by a child below 16 (or 13) with parental authorisation.</td>
<td></td>
</tr>
<tr>
<td><strong>Breach Notification</strong></td>
<td>Data controllers are required to notify the authority of a data breach without undue delay (exceptions apply).</td>
<td>No mandatory requirement, but notification to the Privacy Commissioner (and data subjects, where appropriate) is recommended in the interest of all stakeholders including data users/controllers and subjects.</td>
</tr>
<tr>
<td></td>
<td>Data controllers are required to notify affected data subjects if it is likely to result in high risk to the rights and interests of the data subjects, unless exempted. [Arts 33-34]</td>
<td></td>
</tr>
<tr>
<td><strong>Data Processors</strong></td>
<td>Data processors are additionally obliged to maintain records of processing, ensure security of processing, report data breaches, designate Data Protection Officers, etc. [Arts 30, 32-33, 37]</td>
<td>Data processors are not directly regulated. [s.2(12)]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data users are required to adopt contractual or other means to ensure data processors’ compliance. [DPP2(3) &amp; DPP4(2)]</td>
</tr>
<tr>
<td><strong>New and Enhanced Rights for Data Subjects</strong></td>
<td>• Right to notice on data processing, [Art 13-14]</td>
<td>• Less extensive notice requirements for data users / controllers (processors).</td>
</tr>
<tr>
<td></td>
<td>• Right to erasure of personal data (“right to be forgotten”). [Art 17]</td>
<td>• No right to erasure, but data shall not be retained longer than necessary. [s.26 &amp; DPP 2(2)]</td>
</tr>
<tr>
<td>EU GDPR and HK PDPO (Major Differences) (Cont’d)</td>
<td><strong>EU</strong></td>
<td><strong>HK</strong></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>
| **New and Enhanced Rights for Data Subjects (Cont’d)** | - Right to restriction of processing and data portability. [Art 18, 20]  
- Right to object to processing (including profiling). [Art 21] | - No right to restriction of processing and data portability, but data access and correction requests be complied with. [DPP6, Part 5]  
- No right to object to processing (including profiling), but may opt out from direct marketing activities [ss.35G &35L] and PDPO contains provisions regulating data matching procedure. [ss.30-31] |
| **Certification, Seals, and Codes of Conduct** | Mechanisms are explicitly recognised and established for demonstrating compliance by data controllers and processors. [Art 42] | No formal recognition of certification or privacy seals mechanisms for demonstrating compliance. The Privacy Commissioner may approve and issue code of practice after consultation. [s.12] |
| **Cross-jurisdiction Data Transfer** | Certification and adherence to approved codes of conduct are explicitly made one of the legal bases for transfer. [Art 46] | Certification and adherence to an approved code of practice are not explicitly made a legal basis. |
| **Sanctions** | Data protection authorities are empowered to impose administrative fines on data controllers and processors. [Art 58]  
Depending on the nature of the breach, the fine could be up to €20 million or 4% of the total worldwide annual turnover. [Art 83] | The Privacy Commissioner is not empowered to impose administrative fines or penalties.  
The Privacy Commissioner may serve Enforcement Notices on data users, failure to comply with which may attract penalties after judicial process. [s.50] |
European Union General Data Protection Regulation 2016 (Effective 25 May 2018)

The information and suggestions provided in this publication are for general reference only. They do not serve as an exhaustive guide to the application of the law. The Privacy Commissioner makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information and suggestions set out in this publication. The information and suggestions provided will not affect the functions and powers conferred upon the Privacy Commissioner under the Personal Data (Privacy) Ordinance.

First published in March 2018