

2020年5月修訂版
May 2020 Revised Edition

歐洲聯盟《通用數據保障條例》2016 最新資訊

An Update on European Union General Data Protection Regulation 2016

(於 2018 年 5 月 25 日生效 Effective 25 May 2018)



PCPD



HK



PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

目錄

前言	1
為何《通用數據保障條例》與香港的機構及企業有關？	4
《通用數據保障條例》的域外應用	5
《通用數據保障條例》涵蓋的個人資料	9
新的資料管治、配對及影響評估	10
a. 保障資料主任	10
b. 資料保障影響評估	13
c. 貫徹私隱的設計及預設	14
d. 資料配對	15
敏感個人資料	16
同意	18
a. 「同意」的定義	18
b. 兒童以電子形式表示同意	20
網上服務的提供及cookies的使用	21
資料外洩事故強制通報	23
資料處理者的責任	25
新增及提升的個人權利	28
a. 提升就資料處理方面獲通知的權利	28
b. 提升刪除的權利（「被遺忘權」）	29
c. 提升反對處理的權利	30
d. 新增限制處理的權利	31
e. 新增權利：資料可攜權	32
資料保障印章、行為守則及司法管轄區之間的資料轉移	33
a. 認證／印章及行為守則	33
b. 司法管轄區之間的資料轉移	34
懲罰	35
更多有關《通用數據保障條例》的資訊	37
歐盟的《通用數據保障條例》及香港的《個人資料（私隱）條例》（主要分別）	38

前言

歐洲聯盟（歐盟）二十多年來一直在制定個人資料保障標準方面處於領導地位。歐盟1995年的資料保障指令（**歐盟指令**）¹曾被許多司法管轄區（包括香港）視為基準而依從或參考的法例。歐盟的《通用數據保障條例》²於2018年5月25日在所有歐盟及歐洲經濟區³成員國生效後，訂立了一個前所未有的高標準。《通用數據保障條例》帶來的明顯改革包括新增及提升的個人權利、對資料控制者的問責規定、監管機構的懲處權力，以及條例的域外應用。由於香港與歐盟之間有緊密的經濟連繫，我們於2018年3月首次出版本小冊子，以提高香港各持份者對《通用數據保障條例》可能帶來的影響的認識。今年是《通用數據保障條例》實施兩週年。我們回顧該條例的實施情況及歐盟機關所發出的指引，令小冊子更富資料性。

由於科技發展及全球化，以及歐盟各地就資料保障的基本權利作出憲法上保障，而根據歐盟指令制定的立法框架較為分散，因此《通用數據保障條例》有以下的主要目標及改變：

- 協調及簡化現時的數碼單一市場的框架；
- 讓個人掌握他們的資料；
- 制定現代化的保障資料規範；及
- 基於問責原則的管治。

歐洲資料保障委員會⁴最近發表的一份報告，總結認為《通用數據保障條例》的實施是成功的，因為它「加強了資料保障作為基本權利」⁵。歐盟委員會亦表示，自《通用數據保障條例》實施以來，「市民日益注重他們的權利」⁶。過去兩年，歐洲有關資料保障的投訴大幅上升，就是這些觀點的證明。例如，英國資訊專員公署於2018-19年度接獲超過41,000宗有關資料保障的投訴，升幅幾乎是前一財政年度的一倍⁷。至於歐盟及歐洲經濟區，在2018年5月25日至2019年11月30日期間，監管機構接獲超過275,000宗有關資料保障的投訴。各監管機構接獲的投訴數目差異極大。在《通用數據保障條例》實施的首一年半內，德國和英國分別有超過66,000及64,000宗投訴，位列榜首及次位。第三位的荷蘭有超過37,000宗。但在同一時期，有八個成員國所接獲的投訴個案是低於1,000宗⁸。這些數字或許反映不同成員國的人民對個人資料保障的態度和意識有所差異。在過去兩年，我們亦接獲超過280宗有關《通用數據保障條例》的公眾查詢，以及數宗涉及《通用數據保障條例》、由歐盟人士對香港機構作出的投訴，儘管我們對這些投訴個案並無管轄權。在歐洲有營運業務的香港機構及企業必須保持警惕，留意當地公眾對資料保障的期望已有所提高。

1 1995年10月24日歐洲議會及理事會第95/46/EC號指令涉及處理個人資料及有關資料自由流通的個人保障。

2 2016年4月27日歐洲議會及理事會第2016/679號規例（**歐盟**）涉及處理個人資料及有關資料自由流通的自然人保障，並廢除第95/46/EC號指令。

3 歐洲經濟區包括所有歐盟成員國、冰島、列支敦斯登及挪威。

4 歐洲資料保障委員會是按《通用數據保障條例》成立的獨立歐盟機構，旨在促進執法方面一致與合作。委員會成員包括歐盟成員國國家監管機構的代表及歐洲資料保障監督。

5 歐洲資料保障委員會於2020年2月18日採納的「歐洲資料保障委員會對《通用數據保障條例》第97條的評估」。

6 歐盟委員會於2019年7月24日的新聞稿「《通用數據保障條例》顯成績，但工作仍需繼續」。

7 英國資訊專員公署2018-19年度年報。

8 歐洲資料保障委員會於2020年2月18日採納的「歐洲資料保障委員會對《通用數據保障條例》第97條的評估」。

在循規方面，歐盟委員會留意到「企業正發展出一種循規文化」⁹。調查亦發現個人資料保障已成為很多機構及企業的優先工作之一。歐盟及世界各地的機構，不論大小，已致力確保它們遵從《通用數據保障條例》的規定。個人資料保障已成為管理層要處理的事宜，它有利於營商，並與企業策略及目標緊緊連繫。根據一項在2019年5月進行的調查，歐盟有50萬間機構已根據《通用數據保障條例》登記了保障資料主任¹⁰。私隱管理軟件市場發展蓬勃是另一顯示企業文化轉變的指標。這些轉變的背後動力，包括消費者對私隱期望的提升、《通用數據保障條例》的問責規定，以及違反《通用數據保障條例》的加強懲罰。

在執法方面，歐盟監管機構毫不猶豫地行使新的強大權力，判處行政罰款。根據歐洲資料保障委員會所述，2018年5月25日至2019年11月30日期間，22個歐盟 / 歐洲經濟區成員國的監管機構共判處了785項行政罰款¹¹。根據另一項非官方的調查，截至2020年1月，23個歐盟 / 歐洲經濟區成員國的監管機構共判處了1億1,400萬歐元的行政罰款，以總罰款額計算，法國、德國及奧地利位居榜首¹²。施加罰款的原因有很多，包括欠缺資料保安、保留超乎適度的個人資料，以及沒有就委任保障資料主任通知監管機構。

由於歐盟監管機構有權對一個機構判處的罰款可達其全球年度總營業額的4%，因此有些評論員認為在《通用數據保障條例》的機制下，至今的罰款宗數及數額阻嚇力不足。雖然如此，若假定不經常及低額的罰款是常態，實屬不智。反之，我們應預期日後會有更多的罰款情況，因為監管機構一直在增加其執法隊伍的人手。

除了行政罰款，歐盟監管機構的其他規管權力包括發出循規命令及限制（甚至禁止）處理個人資料。雖然限制或禁止處理個人資料的權力較少被使用（至少以被報道的個案而言），但它對機構或企業更具制肘，因此不容忽視。

至今根據《通用數據保障條例》進行的執法行動大多（如非所有）是針對在歐盟設有永久機關的機構及企業。原因可能是監管機構的資源有限，以及跨司法管轄區執法需要更多努力制定機制。不過，香港機構及企業如屬該條例規管，即使在歐盟沒有實體機關，也不應在循規方面鬆懈。隨著歐盟人士的私隱意識提高及歐盟監管機構的人手逐步增加，規管者可能很快便會嘗試行使其域外權力。香港機構及企業應謹慎評估其營運是否屬《通用數據保障條例》的規管範圍內，如「是」，便要評估是否有遵從《通用數據保障條例》的規定。遵從適用法例畢竟是一項責任，同時亦是企業管治一部分。

9 歐盟委員會於2019年7月24日的新聞稿「《通用數據保障條例》顯成績，但工作仍需繼續」。

10 國際私隱專業人員協會一項調查。

11 歐洲資料保障委員會於2020年2月18日採納的「歐洲資料保障委員會對《通用數據保障條例》第97條的評估」。

12 DLA Piper《通用數據保障條例》資料外洩調查：2020年1月。截至2020年1月，曾根據《通用數據保障條例》施行政罰款的歐盟 / 歐洲經濟區的國家包括（按總罰款額由多至少排列）：法國、德國、奧地利、意大利、保加利亞、西班牙、波蘭、希臘、荷蘭、葡萄牙、挪威、丹麥、羅馬尼亞、英國、捷克共和國、匈牙利、拉脫維亞、塞浦路斯、斯洛伐克、立陶宛、瑞典、比利時及馬爾他；沒有根據《通用數據保障條例》施加任何罰款的歐盟 / 歐洲經濟區的國家包括克羅地亞、愛沙尼亞、芬蘭、冰島、列支敦斯登、盧森堡及斯洛文尼亞。

《通用數據保障條例》的制定亦引發世界各地一輪法例改革潮，包括很多非歐盟國家（例如巴西、印度、馬來西亞、美國及泰國）也制定或建議制定類似規定的資料保障法例。中國內地的《個人信息安全規範》（在個人資料保障方面不具約束力的國家標準）被廣泛認為是在規管上對《通用數據保障條例》的回應。我們在檢討《個人資料（私隱）條例》（香港法例第486章）（**私隱條例**）時，亦曾參考《通用數據保障條例》。全球重整及趨向更高要求的資料保障法律及標準，是大勢所趨。在這個日益連繫緊密的世界營運的機構及企業，應致力達致最高的資料保障標準，以確保能符合不同的規管框架及消費者的期望。長遠來說，不斷選擇合適的規例而搬遷不是可行的辦法。

儘管《通用數據保障條例》已生效兩年，而相關機構亦已發出不少指引，但仍有些難題存在。幾項主要條文需要進一步指引及澄清。例如，第33條有關向監管機構作出資料外洩事故通報的門檻、第42條有關資料處理活動的認證機制，以及第83條有關評估行政罰款的額度。資料外洩事故通報的門檻被認為模糊不清及偏低，加上沒有作出通報可被重罰，因而導致很多微不足道及輕微的資料外洩事故也向監管機構通報，令其資源更形緊絀。認證是《通用數據保障條例》其中一項亮點，因有助展示循規及問責，以及跨司法管轄區的個人資料轉移。不過，認證機制至今似乎仍未制定。不同監管機構就類似的違規情況判處不同程度的行政罰款，亦引起部分人士對一致性及公平性的關注。2019年，德國及荷蘭監管機構就計算行政罰款各自發出指引，以提高罰款的可預測性。不過，歐盟方面仍未有統一罰款額度的指引。

我們更新本小冊子，旨在提供有關《通用數據保障條例》更全面及最新的資訊。然而，本小冊子原旨既不是就《通用數據保障條例》提供法律意見或詮釋，亦不應理解作為《通用數據保障條例》的符規指引。本小冊子的闡述和例子是直接引述《通用數據保障條例》及由官方來源（即歐盟委員會、歐洲資料保障委員會及歐盟監管機構）刊發的相關指引資料。機構及企業應按其所需徵詢具體的法律意見，並對其私隱政策、措施及程序作出適當修訂。

黃繼兒
香港個人資料私隱專員
2020年5月

為何《通用數據保障條例》與香港的機構及企業有關？

在香港，訂立《私隱條例》是為保障個人資料方面的私隱。在草擬《私隱條例》時，曾參考經濟合作及發展組織1980年的私隱指引¹³及歐盟指令。故此，《私隱條例》與歐盟指令有多項共通點。由於《通用數據保障條例》為以歐盟指令為本的資料保障法律帶來了重大的發展及改變，因此新的監管框架內包括了《私隱條例》未有的規定。

《通用數據保障條例》對歐盟以外的資料保障局面帶來的其中一項重大發展，是明確規定在非歐盟法域管轄區內成立的機構在特定的情況下須遵從《通用數據保障條例》的規定。由於業務或交易模式多樣化（例如網上交易），香港的機構及企業必須確定《通用數據保障條例》是否對它們適用，並予以遵從。

13 《經濟合作及發展組織保障私隱及個人資料跨境流通指引》

《通用數據保障條例》的域外應用

香港的機構或企業在以下情況下可能需要遵從《通用數據保障條例》的規定：

- (1) 在歐盟設立機關，而該機關的活動涉及處理個人資料，不論是否確實在歐盟境內處理資料（**機關準則**）；或
- (2) 在歐盟沒有設立機關，但向歐盟人士提供貨品或服務或監察他們的行為（**目標準則**）¹⁴。

《有關《通用數據保障條例》地域範圍（第3條）的第3/2018號指引》¹⁵建議《通用數據保障條例》的地域範圍以上述兩項主要準則為基礎：機關準則及目標準則。該指引進一步指明《通用數據保障條例》第3條旨在決定個別處理活動，而不是個別人士（法人或自然人），是否屬於《通用數據保障條例》的規管範圍之內。因此，某家香港的機構或企業的個別資料處理活動可能屬於《通用數據保障條例》的規管範圍之內，而其他資料處理活動則不屬規管範圍之內。

《通用數據保障條例》非常著重資料處理。《通用數據保障條例》第4(2)條對「處理」所作的定義是「任何對個人資料或連串個人資料進行的運作或連串運作，不論是否以自動化方式進行，例如：收集、記錄、組織、構建、儲存、改編或修改、取回、諮詢、使用、經傳輸、散佈或其他方式公開、調整或結合、限制、刪除或銷毀」。在《通用數據保障條例》下，就處理資料為目的而言，「處理」一詞的定義超越字面的一般意思，當中包括收集、記錄、儲存、改編、披露及刪除。

機關準則

若一家機構或企業在歐盟境內經「穩定的安排」進行「任何實質及有效的活動」（即使是很小的活動），該機構／企業很大機會被視為在歐盟設有機關¹⁶。不過，在歐盟的資料處理者¹⁷不應只憑藉其為代表資料控制者的處理者而被視為該控制者的機關¹⁸。

設立機關的例子：

- ✓ 為向歐盟人士宣傳、售賣、推廣或銷售貨品或服務而設有銷售辦事處
- ✓ 為以上目的委任銷售代理或代表

14 《通用數據保障條例》第3條

15 歐洲資料保障委員會於2019年11月12日採納

16 *Weltimo v. NAIH*, Case C-230/14

17 資料處理者指代表資料控制者處理個人資料的人士或實體

18 《有關《通用數據保障條例》地域範圍（第3條）的第3/2018號指引》

一般來說，《通用數據保障條例》會影響在歐盟設立並以資料控制者及資料處理者¹⁹的角色處理個人資料的機構及企業，不論有關個人資料是否真正在歐盟境內處理²⁰。

有關處理不一定由有關的歐盟機關自己進行。重點是有關處理與該歐盟機關的活動之間是否有密不可分的連繫²¹。

例子：一間營運電子商貿網站的公司以中國內地為基地，資料處理活動只在中國進行。該公司在柏林設有歐洲辦事處，向歐洲市場進行開拓及推廣活動。在柏林的歐洲辦事處的活動與該中國電子商貿網站進行的個人資料處理有密不可分的連繫。

因此該中國公司的個人資料處理可被視為該歐洲辦事處（在歐盟設立的機關）的活動，因而受《通用數據保障條例》的條文規管。

（引自《有關《通用數據保障條例》地域範圍（第3條）的第3/2018號指引》）

根據機關準則，《通用數據保障條例》的應用並不限於處理在歐盟內人士的個人資料。

例子：一間法國公司開發了一個只為摩洛哥、阿爾及利亞和突尼西亞顧客而設的汽車共享應用程式。該服務只在這三個國家提供，但所有個人資料處理活動是由在法國的資料控制者進行。

雖然個人資料是在非歐盟國家收集，但其後的個人資料處理是由在歐盟的資料控制者的機關進行。因此，即使有關的資料當事人不是在歐盟，《通用數據保障條例》仍適用於由該法國公司進行的處理活動。

（引自《有關《通用數據保障條例》地域範圍（第3條）的第3/2018號指引》）

目標準則

即使香港的機構及企業沒有在歐盟設立機關（作為資料控制者或資料處理者），若它們向在歐盟的人士提供貨品或服務或監察其行為時處理他們的個人資料，這些機構及企業也可能會受《通用數據保障條例》影響。

19 《通用數據保障條例》中「資料控制者」的定義與《私隱條例》中「資料使用者」的定義非常相似。《私隱條例》沒有直接規管「資料處理者」，而《通用數據保障條例》則直接對「資料處理者」施加保障個人資料私隱的責任，違規者會被判處行政罰款。本小冊子下文會提供較具體的詳情。

20 見《第29條資料保障工作小組的歐盟《通用數據保障條例》：一般資訊文件》

21 《有關《通用數據保障條例》地域範圍（第3條）的第3/2018號指引》

若要確定機構或企業是否向歐盟人士提供貨品或服務，可視乎它是否明顯地擬向歐盟其中一個或多個成員國的人士提供貨品或服務（不論是否需付款）。就此方面，將會考慮整體情況。

其他因素，例如可採用在一個或多個成員國所使用的語言或貨幣用作訂購貨品及服務，便很可能明顯地表示資料控制者預計向在歐盟的人士提供貨品或服務，或以它們為目標，故受《通用數據保障條例》的規管。

例子：一間日本的網上商店在其網站內以英語介紹產品，並以歐元作結算，一日內處理多宗來自歐盟人士的訂單，並寄送產品給他們。

（引自《第29條資料保障工作小組的歐盟《通用數據保障條例》：一般資訊文件》）

這準則的應用並不受限於其個人資料被處理的人士的公民身份、住處或其他法律地位類別。有關人士的位置才是決定性因素²²。

例子：一間台灣銀行有居於台灣但持有德國公民身份的客戶。這間銀行只在台灣營運，其活動沒有涉及歐盟市場。

這間銀行處理其德籍客戶的個人資料並不受《通用數據保障條例》規管。

（引自《有關《通用數據保障條例》地域範圍（第3條）的第3/2018號指引》）

不過，單是處理歐盟人士的個人資料這點不足以令《通用數據保障條例》適用於非在歐盟成立的機構或企業的處理活動。同時必須有以歐盟人士為「目標」這個元素，不論是向他們提供貨品或服務或是監察他們的行為²³。

例子：一名美國公民假期時途經歐洲。他在歐洲時下載並使用一款由一間美國公司提供的新款應用程式。該應用程式只是針對美國市場。

該美國公司透過該應用程式收集該美國旅客的個人資料並不受《通用數據保障條例》規管。

22 《有關《通用數據保障條例》地域範圍（第3條）的第3/2018號指引》

23 《有關《通用數據保障條例》地域範圍（第3條）的第3/2018號指引》

例子：一所瑞士大學透過網上平台進行碩士課程遴選程序，考生可上載其履歷及聯絡資料。任何具備足夠的德語及英語水平、並持有學士學位的學生皆可參與遴選程序。該大學並沒有特別向歐盟大學的學生作推廣，以及只接受瑞士貨幣作為付款貨幣。

由於這個碩士課程的申請及遴選程序並沒有區別或指明歐盟的學生，因此不能說這所瑞士大學有意圖以某歐盟成員國的學生為目標。足夠的德語及英語水平是適用於任何申請人的一般要求，不論是瑞士居民、歐盟人士或第三國的學生。由於沒有其他因素顯示它特別以歐盟成員國的學生為目標，因此不能說有關處理涉及向歐盟資料當事人提供教育服務，有關處理因而不受《通用數據保障條例》規管。

（兩者均引自《有關《通用數據保障條例》地域範圍（第3條）的第3/2018號指引》）

指派代表

符合目標準則的機構及企業須指派一名在歐盟的代表，豁免條文適用者除外²⁴。

該代表須代表機構或企業與監管機構合作，並與資料當事人溝通。該代表可以是自然人或法人，而且應在資料當事人（其個人資料在向他們提供貨品或服務時被處理或其行為被監察）所處的其中一個成員國內設立。機構或企業的披露責任包括向資料當事人提供其歐盟代表的身份資料²⁵。

例子：一個以土耳其為基地及在當地管理的網站，提供個人化家庭相集的製作、編輯、印刷及派送服務。該網站提供英語、法語、荷蘭語及德語，客戶可以歐元或英鎊付款。該網站指明只可以在法國、比荷盧聯盟及德國以郵遞派送相集。

該網站受《通用數據保障條例》規管，資料控制者必須指派一名在其有提供服務的其中一個成員國（即在法國、比利時、荷蘭、盧森堡或德國）的代表。

（引自《有關《通用數據保障條例》地域範圍（第3條）的第3/2018號指引》）

24 《通用數據保障條例》第27條

25 《有關《通用數據保障條例》地域範圍（第3條）的第3/2018號指引》

《通用數據保障條例》涵蓋的個人資料

《通用數據保障條例》所保障的「個人資料」是指「有關一名已被識別或可被識別的自然人（「資料當事人」）的任何資訊；而一名可被識別的自然人是指可直接或間接地被識別者」²⁶。

《通用數據保障條例》明確列明一系列的識別代號，可屬自然人的個人資料，例如姓名、身份識別號碼、位置資料、網上識別代號，或在參考針對以下方面的一個或多個因素後，可識別該自然人的身份：身體、生理、基因、精神、經濟、文化或社交身份（第4(1)條）。

如一名自然人能夠從其他人被區分出來，該人便是「已識別」或「可識別」。例如，若一名自然人的社交帳戶名稱可將該人從其他人區分出來（不論是否能把「網上」身份與「真實世界」的確實人士聯繫上），其帳戶名稱便是個人資料²⁷。

在決定是否可識別一名自然人，《通用數據保障條例》列明應考慮所有合理地可能被使用的方法²⁸。要確定方法是否屬「合理地可能被使用」，應考慮所有客觀的因素，例如識別行動所需的成本和時間，以及可用的科技²⁹。

在一個根據1995年的歐盟指令裁決的個案中，歐洲法院裁定一個網站營運者（在本案是一個德國政府機構）記錄一名個人進入其網站時的動態互聯網協定地址，構成該人的個人資料，因為該網站營運者能夠以互聯網服務供應商所持有的額外資料，以合法方式識別出該人³⁰。法院的裁決很可能繼續適用於與《通用數據保障條例》有關的個案，因為《通用數據保障條例》對個人資料的定義與1995年的歐盟指令的定義類似，並且較為廣闊。

已去識別、加密或假名化的個人資料，如能夠用來再識別出一個人，仍然是個人資料，受《通用數據保障條例》的規管³¹。

如個人資料已匿名化，無法再從中識別出個人，便不算是個人資料。要資料真正匿名化，匿名程序必須不能逆轉³²。

26 《通用數據保障條例》第4(1)條

27 見英國資訊專員公署出版的《通用數據保障條例》指引：
<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>

28 《通用數據保障條例》敘文26

29 《通用數據保障條例》敘文26

30 *Patrick Breyer v Bundesrepublik Deutschland*, Case C-582/14

31 見歐盟委員會出版的《何謂個人資料？》：https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

32 同上

新的資料管治、配對及影響評估

《通用數據保障條例》第5(2)條明確納入問責原則。機構及企業須(i)展示其遵從處理個人資料的原則；(ii)實施適當的技術性及機構性措施以確保循規；及(iii)在處理的過程中納入對資料的保障³³。

在展示循規方面，機構及企業須考慮資料處理的性質、範圍、內容及目的，以及由此衍生對個人權利和自由的風險。

更具體而言，展示循規並實施或納入資料保障的措施或工具須包括：

- 委任**保障資料主任**監督遵從、履行《通用數據保障條例》及作出相關建議³⁴；
- 進行**資料保障影響評估**，以識別及管理資料保障風險³⁵；
- 採取**貫徹私隱的設計及預設設定**，在決定資料處理方法之時，加入所需的保障措施，確保資料保障原則得以落實³⁶；
- 為資料處理活動保存**記錄**³⁷；及
- 制定資料處理**政策或措施**，以展示循規及問責³⁸。

a. 保障資料主任

《通用數據保障條例》中一項確保循規及問責的重要新措施，是強制性規定須委任保障資料主任。保障資料主任在資料管治系統中擔當重要角色，負責履行問責工具（例如為資料處理活動及政策 / 措施作記錄、進行資料保障影響評估）。歐盟的《**保障資料主任指引**》³⁹就委任保障資料主任、所需的專長及技能提供指引。

33 《通用數據保障條例》第5, 24及25條

34 《通用數據保障條例》第37條（關於適用機構/企業の種類）

35 《通用數據保障條例》第35條

36 《通用數據保障條例》第25(1)條

37 《通用數據保障條例》第30條

38 《通用數據保障條例》第24(2)條

39 由第29條資料保障工作小組發出並於2017年4月5日採納 (http://ec.europa.eu/newsroom/document.cfm?doc_id=44100)

不論機構 / 企業的規模，在下述任何一個情況下均須委任保障資料主任⁴⁰：

- 它是公營機構或團體（法院在行使司法職能時可獲輕微豁免）；
- 其核心活動⁴¹ 包含處理運作時需要對資料當事人作大規模⁴² 的定期及系統性監察⁴³；或
- 其核心活動包含大規模處理敏感個人資料及有關刑事定罪及罪行的資料。

除上述情況，委任保障資料主任屬於自願性質。

估計在《通用數據保障條例》實施的首年，歐盟已有50萬個機構登記了保障資料主任⁴⁴。

保障資料主任至少須執行下述工作⁴⁵：

- 告知及建議控制者 / 處理者及進行資料處理的僱員有關在《通用數據保障條例》下的責任；
- 監察控制者 / 處理者遵從《通用數據保障條例》及資料保障政策的情況，包括分配職責、提高從事資料處理運作的職員之意識並提供培訓，以及進行相關的審核；
- 就資料保障影響評估提供所需的建議，並監察其履行；及
- 與監管機構合作，並擔任聯絡人。

40 《通用數據保障條例》第37(1)條

41 一般來說，「核心活動」可被視為達致資料控制者或處理者的目標的主要運作。這亦包括所有控制者或處理者所進行任何資料處理屬不可分割部分的活動。（見歐盟的《保障資料主任指引》）

42 《通用數據保障條例》沒有為「大規模」下定義，亦難以為此確切訂明受影響資料當事人的數目。不過，歐盟的《保障資料主任指引》列明應考慮下述因素：

- 有關資料當事人的數目；
- 被處理的資料數量及 / 或不同資料項目的範圍；
- 資料處理活動的時期或持續性；及
- 資料處理活動的地理範圍

43 「定期及系統性監察」的典型例子包括網上追蹤、個人概況彙編、信貸評分等活動。

44 根據國際私隱專業人員協會的一項調查

45 《通用數據保障條例》第39(1)條

2019年12月，一個社交媒體平台的德國附屬公司因沒有通知監管機構已委任新的保障資料主任，違反了《通用數據保障條例》第37(7)條，被漢堡資料保障與資訊自由專員判罰51,000歐元。儘管罰款金額不算高，但這個案可警醒資料控制者，委任保障資料主任並把有關委任和保障資料主任的職責通知監管機構，是資料控制者的責任，不應忽視。該社交媒體平台並無就罰款提出上訴，並已繳付罰款。

2019年12月，德國一間小型電訊供應商因沒有依據《通用數據保障條例》第37(1)條委任保障資料主任而被德國聯邦資料保障與資訊自由專員判罰10,000歐元。監管機構表示罰款金額反映該公司多次沒有遵從要求，但罰額不高是基於該公司屬於微企類別。

重要的是，保障資料主任應盡可能在最早階段參與所有涉及資料保障的事宜，並定期出席中、高層會議。當要作出涉及資料保障的決定時，應向保障資料主任尋求意見或邀請其出席，而其意見亦應獲得重視。因此，機構及企業須向保障資料主任提供足夠的資源以執行其職務，不可因履行其職責而受罰或被辭退⁴⁶。保障資料主任所執行的工作及職責不得令其陷入存有利益衝突的情況，尤其是當他擔當高級管理階層的職位或其他需要決定處理個人資料的目的或方式的職責⁴⁷。

雖然現時香港的《私隱條例》並沒有明確提及問責原則及相關的私隱管理工具，惟個人資料私隱專員（**私隱專員**）鼓勵機構及企業採納私隱管理系統以落實問責原則⁴⁸。機構及企業可採用私隱管理系統作為策略性框架，輔以恆常並有效的檢視及監察程序，建立健全的私隱保障基建，藉以協助機構及企業遵從《私隱條例》的規定。私隱管理系統亦有助機構及企業推行公開和具透明度的資訊政策和措施，以示機構及企業有決心體現良好企業管治及建立僱員和客戶之間的信任。委任保障資料主任是私隱管理系統之下建議的其中一種良好行事方式。

46 見歐盟第29條資料保障工作小組的《保障資料主任指引》第3部

47 《通用數據保障條例》第38(6)條

48 見私隱專員發出的《私隱管理系統——最佳行事方式指引》www.pcpd.org.hk/chinese/resources_centre/publications/files/PMP_guide_c.pdf

b. 資料保障影響評估

資料保障影響評估協助資料控制者在初期識別及管理資料保障的風險，避免在較後期才發現問題而引致不必要的費用，改善資料保安，及萬一發生資料外洩事故時保持信任和聲譽。

依據《通用數據保障條例》，資料控制者須在進行任何資料處理之前，基於其性質、範圍、內容及目的可能對個人的權利及自由構成高度風險，而進行資料保障影響評估⁴⁹。尤其是在下述的情況，必須進行資料保障影響評估⁵⁰：

- 以自動化的處理方式，對個人資訊進行有系統及廣泛的評估，包括個人概況彙編，而據此作出的決定會對有關人士產生法律影響或重大影響；
- 大規模處理敏感個人資料或有關刑事定罪或罪行的資料；或
- 有系統地對公共範圍作大規模的監察。

以下例子是須進行資料保障影響評估的情況：

- 機構採用新科技（例如人臉辨識），有系統地監察或追蹤人們的位置或行為；
- 金融機構按信貸資料庫篩選顧客，對顧客的貸款申請作出自動化決定；
- 醫院設立及實施新的健康訊息資料庫，內載病人的健康資料；
- 收集公開的社交媒體資料，以彙編個人概況。

作為良好的行事方式，資料使用者應持續檢視及定期評估資料保障影響評估。資料使用者須謹記，進行資料保障影響評估是持續過程，並非一次性質。

根據《通用數據保障條例》，沒有進行所須的資料保障影響評估，最高可被判罰1,000萬歐元，或全球年度總營業額的2%，以較高者為準。

私隱專員已出版《私隱影響評估》資料單張⁵¹，旨在指導香港的機構及企業就可能對個人資料私隱造成嚴重影響或風險的活動進行評估。私隱專員亦建議資料使用者（或控制者）如在公眾地方或大廈的公共範圍使用閉路電視前，應進行私隱影響評估⁵²。

49 見歐盟第29條資料保障工作小組的《資料保障影響評估指引》，於2017年10月4日採納

50 《通用數據保障條例》第35條

51 見私隱專員的網站：www.pcpd.org.hk/chinese/resources_centre/publications/files/InfoLeaflet_PIA_CHI_web.pdf

52 見私隱專員發出的《閉路電視監察及使用航拍機指引》
www.pcpd.org.hk/tc_chi/resources_centre/publications/files/GN_CCTV_Drones_c.pdf

c. 貫徹私隱的設計及預設

機構及企業須在決定資料處理活動時，實施適當的技術性及機構性措施（例如假名化及數據最少化），以落實執行資料保障原則，並納入所需的保安措施，以符合《通用數據保障條例》的規定⁵³。

就貫徹資料保障的設計，可考慮下述因素：

- 處理資料的性質、範圍、內容及目的；
- 對個人的權利及自由所構成的風險程度；
- 技術發展；及
- 實施的成本。

此外，須預設適當的技術性及機構性措施，確保所處理的個人資料是為個別特定目的所需的。這規定適用於所收集的資料數量、處理的規模、儲存時期及資料的存取程度⁵⁴。

2019年11月13日，歐洲資料保障委員會發出《有關第25條貫徹資料保障的設計及預設的第4/2019號指引》草擬稿⁵⁵，就保障資料原則提供如何實行貫徹資料保障的設計及預設的實用指引和例子。例如，在透明原則方面，私隱政策（包含資料控制者如何收集、使用及共用個人資料的資訊）須可供所有人查閱，包括使用機器可讀語言，提高可讀性及清晰程度。私隱政策亦應在不同渠道及媒體提供，不只限於文字，以便有效地傳遞予資料當事人。在公平原則方面，個人資料處理的預設選項必須是私隱侵犯程度最低的，而進一步處理的選擇的呈示方式不得阻撓資料當事人選擇放棄。如採用演算法分析及預測資料當事人，須充分知會他們。

懲罰

2019年10月30日，德國一間地產公司因(i)保留租戶的個人資料大幅超過所需時間及(ii)違反貫徹資料保障的設計規定，被柏林資料保障與資訊自由專員判罰1,450萬歐元⁵⁶。監管機構在2017年6月及2019年3月實地視察時，發現該公司採用封存系統儲存租戶的個人資料，而該系統並不提供刪除不需要的資料的選項。該公司儲存租戶的個人資料（包括銀行結單、糧單、僱傭及培訓合約摘錄、稅務、社會保障及健康保險資料），卻沒有檢查有關儲存是否獲容許或有需要。罰款金額高昂，是因為監管機構認為該地產公司蓄意設立該資料系統，並長時間不當地處理資料。

53 《通用數據保障條例》第25(1)條

54 《通用數據保障條例》第25(2)條

55 這指引草擬本的公眾諮詢已於2020年1月16日結束。

56 截至2020年3月，有關決定未屬最終決定，因為該地產公司已表明會提出上訴。

2019年10月11日，一間教育機構亦因手機應用程式處理個人資料的保安欠佳而被挪威監管機構判罰12萬歐元⁵⁷。該應用程式是用作學校僱員、家長與學生之間的溝通，當中會處理特別類別的個人資料，例如兒童的健康資料。該應用程式的保安欠佳，令未獲授權人士得以進入及改動超過63,000名學生的個人資料。監管機構認為這是因為該應用程式在推出前沒有進行足夠的保安測試。這個案提醒機構在研發過程中加入保安測試的時間及經費，並支援保安測試（這是貫徹私隱的設計及預設的概念）。在推出應用程式前進行保安測試，有助發現及評估應用程式被未經授權進入的風險，從而實施足夠的認證控制措施。

d. 資料配對

機構及企業（作為資料控制者或處理者）須保存其資料處理活動的記錄，包括處理的資料種類、使用資料的目的、轉移個人資料至第三國或國際機構／企業等⁵⁸。

僱用少於250人的機構及企業可獲豁免，除非(i)其資料處理活動很可能對資料當事人的權利及自由帶來風險，(ii)其核心活動涉及處理敏感個人資料、有關刑事定罪及罪行的個人資料或有系統的大規模監察活動⁵⁹。

機構及企業可為其資料處理活動設計範本作盤點及分類用途。在設計適合的範本時，應採用簡潔精確的語言，並輔以解釋。有關記錄必須定期予以檢視，以確保資料獲得更新。這重要步驟可協助保障資料主任或機構及企業評估接著應如何達致資料保障的管治。

機構及企業亦應制定適當的保障個人資料政策及措施，讓員工可以遵從。

雖然《私隱條例》沒有明確規定要保存記錄，但香港的機構及企業須令其私隱政策及措施具透明度⁶⁰。私隱管理系統的其中一個重要部分是資料使用者備存個人資料庫存，讓機構及企業可以小心地檢視他們所持有的個人資料及他們現時是如何處理資料。

57 監管機構原本判罰20萬歐元，但最後因有緩減因素而將金額降至12萬歐元，包括該教育機構實施措施迅速減低損失及表示願意解決問題。

58 有關記錄的其他詳情，請參閱《通用數據保障條例》第30(1)及(2)條

59 《通用數據保障條例》第30(5)條

60 《私隱條例》附表1保障資料第5原則

敏感個人資料

《通用數據保障條例》就處理特別類別的個人資料，較歐盟指令施加較嚴格的規定⁶¹。這些類別的個人資料基於其固有及不可改變的性質，被視為本質較為敏感，又或基於不當的處理可能會為個人造成嚴重傷害或歧視性後果而作出劃分。

根據《通用數據保障條例》，「特別類別」的個人資料是指揭示種族或民族本源、政治意見、宗教或哲學信仰、工會會籍的個人資料、有關健康狀況的資料或有關一名自然人的性生活或性取向的資料，及為單獨識別一名自然人而處理的基因資料或生物辨識資料。（與歐盟指令相比，（間線者）屬新增項目）

《通用數據保障條例》禁止處理這些特別類別的個人資料，除非符合其中一項指明的條件，當中包括(i)資料當事人就有關處理已經給予明確的同意；(ii)為了重大的公眾利益，有關處理屬必需的，亦與所追求的目標相稱；或(iii)為了公眾健康方面的公眾利益，有關處理屬必需的，例如防止嚴重的跨境健康威脅等等⁶²。

2020年3月，2019冠狀病毒全球爆發，引起在歐盟不同地區對抗冠狀病毒時使用及處理個人資料的私隱關注。在歐洲資料保障委員會於2020年3月19日採納的《在2019冠狀病毒全球爆發中處理個人資料的聲明》中，委員會表示根據歐盟或成員國的法律，為了公眾健康方面的重大公眾利益⁶³，處理某些特別類別的個人資料（例如健康資料）屬必需的；或正如《通用數據保障條例》敘文46特別提及在控制疫情時，處理個人資料是有需要保障資料當事人的重要利益⁶⁴，這些情況可豁免遵守有關禁止處理某特別類別的個人資料的規定。在對抗冠狀病毒全球大流行中，歐洲資料保障委員會認為資料保障規例（例如《通用數據保障條例》）不應阻礙對抗病毒的措施，但資料控制者仍須確保個人資料私隱的保障，並保證合法處理個人資料。在緊急情況下，限制自由可被合法化，惟有關限制程度須屬相稱及只限於緊急期間。

61 《通用數據保障條例》第9條

62 有關其他界定敏感個人資料的條件，請參閱《通用數據保障條例》第9(2)條

63 《通用數據保障條例》第9(2)(i)條

64 《通用數據保障條例》第9(2)(c)條

有關收集敏感個人資料的懲罰

2019年8月20日，瑞典一所中學因收集學生容貌影像（被視為敏感資料）作出席記錄，被瑞典監管機構判罰20萬瑞典克朗（約為18,630歐元）。監管機構認為，由於學校與學生之間的關係並不對等，而且出席記錄是單方面的控制措施，因此學生或家長的同意不能被視為自願，這不屬自願的同意亦不能用來作為豁免禁止使用學生的敏感個人資料的法律根據。因此，該校違反了《通用數據保障條例》第9條。此外，監管機構亦裁定使用人臉辨識技術與目的（即記錄出席）不相稱，而且記錄出席情況可以較不侵犯私隱的方式進行。

2019年12月17日，一間在倫敦的藥房沒有確保特別類別資料的保安，違反了《通用數據保障條例》，被英國資訊專員公署判罰275,000英鎊。該藥房將約50萬份文件（載有姓名、地址、出生日期、國民保健服務編號、醫療資料及處方）放在沒有上鎖的櫃內。

在歐洲資料保障委員會採納的一份有關《經視頻裝置處理個人資料的指引》⁶⁵中，委員會列出一些處理特別類別資料時（例如以具有人臉辨識技術的視像監察系統來識別一名人士）需考慮的因素。首先，資料控制者必須有根據《通用數據保障條例》第9條處理特別類別資料的例外情況（即限制處理特別類別資料的一般規定的相關豁免情況）及根據第6條處理資料的法律基礎。以人臉辨識技術處理生物辨識資料會對資料當事人的權利帶來更大的風險，因此需要對某些責任持續加強警覺，例如更高的保安程度及進行資料保障影響評估（如有需要）。企業為其商業目的而安裝包括臉容或其他生物辨識資料的視頻監察系統，一般需要取得所有人士的明確同意。

香港的《私隱條例》沒有就被視為敏感類別的個人資料施加較嚴格的規定。不過，《私隱條例》規定機構及企業在考慮實施適當措施確保資料保安時，須考慮個人資料的種類⁶⁶。因此，機構及企業應採取與個人資料的敏感程度相稱的保障或保安措施。私隱專員出版的《為收集及使用生物辨識資料指引》⁶⁷為收集及使用生物辨識資料（因其獨特性及與資料當事人的健康、精神狀況或種族本源有密切關係而被視為敏感資料）的資料使用者提供指引，並建議良好的行事方式。

65 歐洲資料保障委員會於2020年1月29日採納的有關經視像裝置處理個人資料第3/2019號指引

66 見《私隱條例》附表1保障資料第4原則

67 見私隱專員網站：https://www.pcpd.org.hk/chinese/resources_centre/publications/files/GN_biometric_c.pdf

同意

根據《通用數據保障條例》，資料當事人的「同意」是合法處理個人資料的法律基礎之一。

概括而言，《通用數據保障條例》下合法處理個人資料的基礎包括⁶⁸：

- 資料當事人同意就個別或多個特定目的作處理；
- 履行與資料當事人的合約或採取步驟為這合約作準備；
- 依從法律責任；
- 保護資料當事人或另一人的重要利益，而資料當事人無能力給予同意；
- 執行為公眾利益而進行的工作或行使賦予資料控制者的正式權力；
- 為合法利益為目的。

a. 「同意」的定義

《通用數據保障條例》把「同意」定義為資料當事人自由給予的具體、知情及不含糊的指示，以聲明或清晰肯定的行動表明同意處理其個人資料⁶⁹。（間線標示強調）

當機構及企業以書面聲明的形式向資料當事人徵求同意時，須以清晰簡單的語言、容易明白及讀取的方式，並且獨立地展示此要求⁷⁰。除了基本資料（例如資料控制者的身份及將收集及使用的資料類別），資料當事人亦應獲告知他們有權撤回其同意。

有效及無效同意的例子：

- ✗ 個人不獲允許就不同的個人資料的處理運作個別地給予同意
- ✗ 網綁式同意的情況是指有關同意需要連同其他不必要的處理活動一併作出，以作為履行服務合約的條件
- ✗ 在空格預設剔號，同意條款及細則
- ✗ 資料當事人保持緘默或沒有行動
- ✓ 瀏覽網站時加上剔號表示同意特定的資料處理用途
- ✓ 在智能電話安裝應用程式選擇技術設定
- ✓ 清楚表明拒絕或撤回同意不會引致服務被拒

68 《通用數據保障條例》第6(1)(a)至(f)條

69 《通用數據保障條例》第4(11)條

70 《通用數據保障條例》第7條

資料控制者必須確保同意可以如被給予時那般容易被撤回及可在任何指定時間被撤回⁷¹。如某個人撤回同意，資料控制者必須停止有關處理，不能轉用同意以外的其他法律基礎⁷²。有關取得及展示有效同意的詳細說明及規定，請參閱《第29條工作小組有關第2016/679號規例的同意指引》⁷³。

自《通用數據保障條例》實施以來，有些資料控制者因在沒有有效的同意下處理個人資料而須負上責任。例如：

- 一間環球網絡搜尋引擎公司因沒有為其個人化廣告有效地取得資料當事人的同意（例如使用預剔格子，就其所有處理運作取得全面同意），被法國監管機構判罰5,000萬歐元；
- 一間能源零售公司因未經顧客同意而作出電話推廣，及向未取得披露資料同意的機構索取潛在顧客的資料，被意大利監管機構判罰850萬歐元；
- 一間環球會計及核數事務所因在不適當的同意基礎下處理僱員的個人資料，被希臘監管機構判罰15萬歐元，因基於勞資雙方明顯不對等的關係，僱員的同意一般不能被視為屬自由給予⁷⁴。

71 《通用數據保障條例》第7(3)條

72 《第29條工作小組有關第2016/679號規例的同意指引》第6部

73 歐洲資料保障委員會於2018年5月核准

74 《第29條工作小組有關第2016/679號規例的同意指引》第3.1.1部

b. 兒童以電子形式表示同意

機構及企業就處理兒童的個人資料以提供「資訊社會服務」⁷⁵（例如電子商貿企業、提供網上資訊的網上市場、搜尋器提供的互聯網參考服務等）而徵求兒童的同意時，必須特別小心。根據《通用數據保障條例》，任何16歲以下的兒童（或部分歐盟成員國定為13歲），其同意必須由負有父母責任的人士給予或授權⁷⁶。

在香港，雖然《私隱條例》沒有明確規定收集個人資料需要以同意作為基礎之一，但機構及企業須把收集目的告知當事人；如將個人資料用於與原本收集目的無直接關係的用途或直接促銷用途時，則須取得他們的「訂明同意」。「訂明同意」是指自願給予的明確同意，並且沒有以書面撤回。私隱專員的規管立場是，同意必須是知情地給予，並不是從沒有行動或緘默之下而推斷的。同樣地，私隱專員強調，機構及企業的良好行事方式是應向個人提供選擇，不要將給予同意的情况，與提供服務無關的其他條款或細則網綁在一起。

至於任何一名處於弱勢的資料當事人並屬於(i)未成年人⁷⁷，(ii)無能力處理其本身事務，或(iii)精神上無行為能力的人士，《私隱條例》容許藉由「有關人士」⁷⁸在有合理理由相信將有關資料用於新目的明顯是符合該資料當事人的利益⁷⁹的情況下，代他給予訂明同意。

75 根據2015年9月9日歐洲議會及理事會第2015/1535號指令第1(1)(b)條，「資訊社會服務」的定義是「任何按接受服務者的個別要求、以電子方式遙遠地為了收取報酬而提供的一般性服務」。

76 《通用數據保障條例》第8條

77 《私隱條例》沒有對「未成年人」訂明具體的定義，但在香港特區法律下，一名「未成年人」是指一名18歲以下的人士（見《釋義及通則條例》（第1章）第3條。根據《成年歲數（有關條文）條例》（第410章），年滿18歲的人士屬於成年）。

78 「有關人士」包括(i)未成年人的父母；(ii)由法庭委任以處理其事務的人或(iii)精神上無行為能力的人的監護人（《私隱條例》第2(1)條）。

79 《私隱條例》附表1保障資料第3(2)原則

網上服務的提供及cookies的使用

網上服務已成為日常生活的重要部分，網上服務供應商常為定向廣告及個人化內容等目的進行用戶行為追蹤。在歐盟設有機關或以歐盟人士為目標的機構及企業應確保其網站以公平及透明的方式處理個人資料，符合目的限制及資料最小化的責任，以及具備法律基礎（例如資料當事人的同意、為履行合約所必需等）。

根據《向資料當事人提供網上服務時根據《通用數據保障條例》第6(1)(b)條處理個人資料的第2/2019號指引》⁸⁰，《通用數據保障條例》第6(1)(b)條下的「為履行合約所必需」的概念⁸¹不是純粹評估合約條款容許或列明的事項。資料控制者應就其目的對資料處理活動進行以事實為基礎的評估，並就達致相同目的而言，它是否較其他選項具較低的侵犯程度。

例子：一名資料當事人向網上零售商購買貨品。該資料當事人希望以信用卡付款及在其住址收取貨品。要履行合約，該零售商為結算目的必須處理該資料當事人的信用卡資料及賬單地址，及為送貨目的而處理該資料當事人的住址。因此，《通用數據保障條例》第6(1)(b)條可作為這些處理活動的法律基礎。

不過，如該顧客選擇送貨至一個取貨點，則處理其住址不再是履行該購買合約所必需。在這情況下，任何對該資料當事人的住址的處理必須有另一個法律基礎。

（引自《向資料當事人提供網上服務時根據《通用數據保障條例》第6(1)(b)條處理個人資料的第2/2019號指引》）

除非屬構成某些網上服務的固有及預期的元素，否則內容個人化並不被視為履行合約所必需⁸²。在這情況下，資料控制者應考慮其他適用的法律基礎。

例子：一個網上酒店搜尋引擎監察用戶過往的訂房記錄，以彙編其典型支出概況。這概況資料其後在提供搜尋結果時，用作向用戶建議某些酒店。在這個案，彙編用戶的過往行為及財務資料在客觀上並不是履行合約所必需，即根據用戶所提供的特定搜尋準則提供款待服務。因此，《通用數據保障條例》第6(1)(b)條不是這處理活動的適用基礎。

（引自《向資料當事人提供網上服務時根據《通用數據保障條例》第6(1)(b)條處理個人資料的第2/2019號指引》）

80 歐洲資料保障委員會於2019年10月8日採納

81 《通用數據保障條例》第6(1)(b)條的基礎是「處理是履行合約所必需的，而資料當事人是該合約的一方，或有關處理是按資料當事人要求採取以達成合約的步驟」。

82 見《向資料當事人提供網上服務時根據《通用數據保障條例》第6(1)(b)條處理個人資料的第2/2019號指引》第3節

現時，機構及企業經常利用cookies（儲存於電腦或流動裝置的小型文字檔案），追蹤網站用戶的網上活動。除了網站營運者直接使用的第三方cookies，亦有第三方cookies，通常由廣告商使用，以建立用戶的概況資料及進行定向廣告。網上身份標識符（例如互聯網協定地址及cookie身份標識符）會被用作建立個人的概況資料及識別個人⁸³。因此，根據《通用數據保障條例》，使用cookies可構成處理個人資料。

英國、法國、德國及西班牙的監管機構分別發出使用cookies及其他網絡追蹤技術的指引。例如英國資訊專員公署在《使用cookies及類似技術的指引》⁸⁴中指出，一個人持續使用一個網站並不構成有效的同意，以及不能對非必要的cookies使用預剔格子。

歐洲法院在2019年10月一宗有關博彩網站使用cookies的案件⁸⁵肯定了上述的觀點。雖然這個案是基於《電子私隱指令》⁸⁶（旨在為電子通訊業處理個人資料，就《通用數據保障條例》作出具體說明及補充）⁸⁷，但法院參考了《通用數據保障條例》下的「同意」概念。法院裁定網站營運者在使用非必要的cookies（例如推廣cookies）前，用戶必須已主動選擇給予指明同意。預剔格子讓用戶取消選擇或拒絕同意的做法並不足夠。

雖然在科技中立的《私隱條例》中沒有關於網上身份標識符或電子通訊的特定條文，但私隱專員已出版多份有關資訊及通訊科技的私隱議題的資料單張，以供公眾參考，例如《機構智用社交網絡 尊重個人資料私隱》、《網上行為追蹤》、《保障個人資料私隱：流動應用程式開發商及其委託人須知》⁸⁸。

83 《通用數據保障條例》敘文30列明：「自然人可能與他們的裝置、應用程式、工具及通訊協定所提供的網上身份標識符有連繫，例如互聯網協定地址、cookie身份標識符或其他身份標識符，例如射頻識別標籤。這會留下足跡，尤其是與獨特的身份標識符及伺服器收取的其他資訊結合後，可用來彙編自然人的概況，並識別他們。」

84 見：<https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf>

85 *Verbraucherzentrale Bundesverband e.V. v. Planet49 GmbH*, Case C-673/17

86 由第2006/24/EC號指令及第2009/136/EC號指令修訂2002年7月12日歐洲議會及理事會有關電子通訊業處理個人資料及保障私隱的第2002/58/EC號指令（電子私隱指令）。

87 見《歐洲資料保障委員會有關電子私隱指令與《通用數據保障條例》的相互作用，尤其關於資料保障機構的能力、工作及權力的第5/2019號意見書》。

88 見私隱專員的網站：https://www.pcpd.org.hk/chinese/resources_centre/publications/information_leaflet/information_leaflet.html

資料外洩事故強制通報

《通用數據保障條例》⁸⁹強制規定機構及企業通報資料外洩事故，而它們須根據《通用數據保障條例》向歐盟成員國的監管機構通報資料外洩事故，不可延誤（如情況許可，應在得悉事件後不多於72小時內通報），除非有關事故不大可能對個人的權利及自由構成風險。如有關事故很可能對受影響人士的「權利及自由造成高度風險」，須通知受影響人士，除非情況獲得豁免⁹⁰。作為資料處理者的機構及企業亦須負上同樣的責任。

向監管機構發出的資料外洩事故通報所規定的內容包括⁹¹：

- 事故的性質及可能或實際的後果；
- 資料當事人及有關個人資料的類別及大約數目；
- 已採取或擬採取的措施，以減低事故造成的不利影響；及
- 機構或企業的保障資料主任或其他聯絡人的聯絡資料。

正如《第2016/679號規例的個人資料外洩事故通報指引》⁹²及《歐盟機構及團體適用的個人資料外洩事故通報指引》⁹³建議，資料外洩事故通報責任是以「風險為本」為基礎，事故的嚴重性須按每宗個案而評估。在評估是否對「個人的權利及自由造成風險」時，須考慮下述因素：

- 事故的種類；
- 個人資料的性質、敏感程度及數量；
- 識別有關人士的容易程度；
- 對個人造成的後果的嚴重性；
- 受影響人士的特別特徵；
- 資料使用者的特別特徵；及
- 受影響人士的數量。

上述每項因素須逐一小心評估或與其他因素綜合評估，以衡量對個人造成的風險程度。

89 第33條

90 根據《通用數據保障條例》第34(3)條，在下述情況，無須向受影響資料當事人通報：
(a) 已有適當的技術性及機構性保障措施，尤其是所採取的措施令非獲授權人士無法理解資料（例如加密）；
(b) 資料控制者其後已採取措施，確保所預期對資料當事人的權利及自由造成的高度風險不太可能發生；或
(c) 若涉及不相稱的資源，則可以公開形式告知資料當事人作為替代方案。

91 《通用數據保障條例》第33-34條及敘文85-86

92 由第29條工作小組發出，並於2018年2月6日採納。

93 歐洲資料保障監督於2018年11月21日發出。

下述個人資料外洩事故例子是符合向監管機構及受影響的資料當事人作出通報的門檻：

- ✓ 大量學生的個人資料被錯誤地發送予超過一千個收件者
- ✓ 一間醫院的醫療記錄因為網絡攻擊而30小時不能被查取
- ✓ 載有告密過程資訊的資料庫被黑客入侵，在互聯網上被公開。告密者及有關人士的姓名亦被公開
- ✓ 一間公司遭勒索軟件攻擊，令登記參與一個融資計劃的市民的所有個人資料被加密。公司沒有備份資料，有關資料亦不能復原

2019年5月，匈牙利一個政黨因沒有根據《通用數據保障條例》第33(1)條及34(1)條通知監管機構及受影響人士一宗資料外洩事故，及沒有根據《通用數據保障條例》第33(5)條記錄事故的經過、其帶來的影響及所採取的補救行動，被匈牙利國家資料保障與資訊自由管理局判罰1,100萬匈牙利福林（32,000歐元）。該事故是因黑客對機構的系統進行網絡攻擊，洩露了超過六千名人士的資料（例如姓名，電郵及密碼）。

在香港，資料外洩事故通報屬自願性質。私隱專員出版了《資料外洩事故的處理及通報指引》⁹⁴，闡述作出通報的行動。私隱專員建議機構及企業的良好行事方式是盡快通知私隱專員及任何受影響人士，讓他們可立即採取行動以減低任何可能的傷害。

94 見私隱專員的網站：www.pcpd.org.hk/chinese/resources_centre/publications/files/DataBreachHandling2015_c.pdf

資料處理者的責任

擔當資料處理者的香港機構及企業（例如於歐盟成立的企業所聘請分析個人資料的服務提供者、雲端服務提供者等，而只用於企業所指明的目的），可能受《通用數據保障條例》內的新增及廣泛的規定所影響。

首先，《通用數據保障條例》規定資料控制者須委任或揀選在技術性措施及機構性措施方面可提供足夠保證的資料處理者，令相關的資料處理活動符合《通用數據保障條例》的要求，並確保資料當事人的權利得到保障⁹⁵。此外，資料控制者須採取合約方式或法律步驟，對處理者作出相關約束。《通用數據保障條例》提供了具體條文須納入這類合約內⁹⁶：

- 只按控制者的書面指示而處理個人資料；
- 確保獲授權處理個人資料的人士致力保密或負上適當的法定保密責任；
- 確保所處理的個人資料的安全；
- 聘用另一處理者時依從指定的條件；
- 協助控制者回應資料當事人行使《通用數據保障條例》所賦予的權利（例如第III章內的資料查閱權、修改權等）所作出的要求；
- 協助控制者遵從資料保安及資料保障影響評估的責任；
- 在資料處理活動結束後，按控制者的選擇刪除或交還所持有的個人資料，並刪除現有複本，除非法律規定須儲存有關資料；及
- 向控制者提供能顯示已履行責任所需的資訊，並讓控制者進行審核，包括視察。

2018年12月，德國一間小型船務公司因沒有遵守《通用數據保障條例》第28(3)條與其服務供應商（作為資料處理者）簽訂處理合約，列明服務供應商所採取的保安措施及它們如何遵從《通用數據保障條例》的標準，被漢堡資料保障與資訊自由專員判罰5,000歐元。在沒有簽訂處理合約的情況下，監管機構認為該公司在沒有恰當的法律根據下把敏感資料傳送予該服務供應商。另一個加重刑罰的因素是儘管該公司知道其在《通用數據保障條例》下的責任，但有關的不恰當做法仍持續一段時間，並故意不採取步驟作出糾正。

95 《通用數據保障條例》第28條

96 《通用數據保障條例》第28(3)條

《通用數據保障條例》亦對資料處理者施加直接的責任，包括（但不限於）⁹⁷：

- 未獲控制者的授權，不得聘用另一處理者；
- 保存資料處理活動的記錄；
- 執行任務時，應監管機構要求與之合作；
- 除非屬法律規定的情況，否則按控制者的指示進行處理；
- 確保資料處理活動的安全；
- 向控制者通報資料外洩事故，不可延誤；
- 委任保障資料主任；及
- 只在訂明的條件下把個人資料轉移至歐盟以外的地方。

就保存記錄的規定而言，《通用數據保障條例》對僱用少於250人的機構及企業提供局部的豁免。此外，歐盟成員國的監管機構在應用《通用數據保障條例》時，獲鼓勵考慮中小微企業⁹⁸的特點。

根據《通用數據保障條例》，資料處理者是直接受監管機構所規管，違反責任（例如沒有通報資料外洩事故）可被判罰⁹⁹。直接規管令資料處理者對個人資料保安、保留及使用採取與資料使用者同等程度的謹慎和小心。

有關《通用數據保障條例》的《地域範圍（第3條）的第3/2018號指引》進一步釐清了《通用數據保障條例》對歐盟以外的資料處理者的適用情況¹⁰⁰。要考慮非歐盟處理者是否受《通用數據保障條例》規管，必須視乎該處理者的處理活動是否與控制者以在歐盟內的人士為目標的活動相關。如控制者的處理活動關乎向在歐盟內的人士提供貨品或服務或監察在歐盟內的人士的行為（即以在歐盟內的人士為目標），被指示代表該控制者進行該處理活動的任何處理者，將根據《通用數據保障條例》第3(2)條而受《通用數據保障條例》所規管。

97 有關資料處理者的直接責任，見《通用數據保障條例》第28(2)條；敘文82；第30(2)條；第30(4)條；第31條；第29條；第32(1)條；第33(2)條；第37(1)條；第45-47條及第49條。

98 歐盟委員會刊發的委員會建議第2003/361/EC號指令的附錄第2條述明：

(1) 中小微企業是由僱用少於250人及年度營業額不超過五千萬歐元及 / 或年度資產負債表的總額不超過四千三百萬歐元。
 (2) 在中小微企的類別下，小型企業的定義是僱用少於50人及年度營業額及 / 或年度資產負債表的總額不超過一千萬歐元。
 (3) 在中小微企的類別下，微型企業的定義是僱用少於10人及年度營業額及 / 或年度資產負債表的總額不超過二百萬歐元。

99 《通用數據保障條例》第58, 77, 79, 82及83條

100 歐洲資料保障委員會於2019年11月12日採納

例子：一間美國公司（作為資料控制者）開發了一個健康與生活方式的應用程式，收集及分析用戶的睡眠時間、體重、血壓、心跳等，以提供健康建議。這個應用程式是提供予在歐盟內的人士使用。為了儲存資料，該美國公司聘用了一個在美國的雲端服務供應商作為處理者。

由於該美國公司營運該健康與生活方式應用程式是監察在歐盟內的人士的行為，其處理屬於《通用數據保障條例》第3(2)條下的規管範圍。該雲端服務供應商在根據該美國公司的指示及代該美國公司進行處理時，該雲端服務供應商是進行「關乎」其控制者以在歐盟內的人士為目標的處理活動。處理者代其控制者進行的這個處理活動，根據《通用數據保障條例》第3(2)條是屬於《通用數據保障條例》的規管範圍。

（引自《有關《通用數據保障條例》地域範圍（第3條）的第3/2018號指引》）

在香港，只作為資料處理者¹⁰¹的機構及企業，並不直接受《私隱條例》¹⁰²規管。不過，它們仍負有間接責任，其作為資料使用者的主事人，須採取合約或其他方式，以(i)防止轉移予資料處理者的資料被保留超過處理所需的時間，及(ii)防止資料被未獲准許的或意外的查閱、處理、刪除、喪失或使用¹⁰³。其主事人須就處理者在其明示或暗示授權下，代他們所作出的違規行為或作為負上責任¹⁰⁴。關於外判活動的資料保障，私隱專員出版了《外判個人資料的處理予資料處理者》資料單張，在合約及非合約的措施¹⁰⁵方面，為機構／企業提供建議。

101 資料處理者是指符合以下兩項說明的人：(a)代另一人處理個人資料；及(b)並不為該人本身目的而處理該資料。（《私隱條例》保障資料第2(4)原則）。

102 根據《私隱條例》第2(12)條，如某人純粹代另一人持有、處理或使用的任何個人資料，而該首述的人並非為其任何本身目的而持有、處理或使用（視屬何情況而定）該資料，則（但亦只有在此情況下）該首述的人就該個人資料而言不算是資料使用者。

103 依據《私隱條例》附表1保障資料第2(3)及4(2)原則

104 《私隱條例》第65(2)條

105 見私隱專員的網站：www.pcpd.org.hk/chinese/resources_centre/publications/files/dataprocessors_c.pdf

新增及提升的個人權利

《通用數據保障條例》維護、加強及進一步提升個人各方面的權利（包括資訊、查閱、修改、反對、限制、刪除、被遺忘權、及資料可攜權）。

a. 提升就資料處理方面獲通知的權利

除卻一些例外情況¹⁰⁶，《通用數據保障條例》規定機構及企業向個人提供一系列有關處理其個人資料的訂明資訊。訂明資訊必須以精確、具透明度、容易明白及讀取的方式展示。因此，機構及企業應檢視其《收集個人資料聲明》或私隱政策及措施，以遵從《通用數據保障條例》對加強個人的通知權利方面的規定。

一般來說，訂明資訊包括¹⁰⁷：

- | | | |
|---|--|--|
| <ul style="list-style-type: none"> 資料控制者的身份及聯絡資料、保障資料主任（如已委任）的聯絡資料 資料處理的目的及基礎（例如處理資料的合法利益） 撤回同意的權利（如資料處理是基於同意）及反對有關處理的權利 | <ul style="list-style-type: none"> 資料接收者的類別 保留時期 刪除權 對個人作出自動化的決策及其背後邏輯 向相關監管機構投訴的權利 | <ul style="list-style-type: none"> 提供資料是否屬強制性及不提供的後果 司法管轄區之間作出資料轉移的資訊 資料來源（如資料非向個人收集） |
|---|--|--|

在香港，雖然機構及企業向個人直接收集其個人資料時須告知他們某些資訊，而它們在這方面的私隱政策及措施必須具透明度¹⁰⁸，惟《私隱條例》在向個人提供訂明資訊方面所要求的項目相對較少。《通用數據保障條例》明確規定，即使個人資料不是直接從個人收集，亦需給予通知，除非屬有限的例外情況¹⁰⁹。

¹⁰⁶ 根據《通用數據保障條例》第14(5)條，例外情況可概括為：(1)資料當事人已得悉有關資訊；(2)所需作出的資源並不相稱；(3)法律容許披露，並已採取措施保障資料當事人的合法權益；及(4)保密責任。

¹⁰⁷ 《通用數據保障條例》第13及14條

¹⁰⁸ 《私隱條例》附表1保障資料第1(3)及5原則

¹⁰⁹ 《通用數據保障條例》第14條

私隱專員鼓勵香港的機構及企業在處理資料的措施上具透明度。此外，如作出有關通知很可能損害《私隱條例》第8部所載的目的，《私隱條例》載有條款（即《私隱條例》附表1保障資料第1(3)原則）豁免收集資料時的通知規定¹¹⁰。

b. 提升刪除的權利（「被遺忘權」）

《通用數據保障條例》的刪除權（亦稱「被遺忘權」）¹¹¹讓個人在指定情況下有權要求機構及企業刪除其個人資料，不可延誤，包括(i)就收集目的而言，有關個人資料已不再需要，(ii)該個人撤回同意（而資料處理活動是建基於其同意），(iii)沒有凌駕性的合法利益，或(iv)所收集的個人資料是關於接受資訊社會服務的兒童等。

倘資料控制者公開披露個人資料（例如在互聯網上披露），須採取合理的步驟（考慮到現有科技及實施成本），通知正處理資料的其他控制者（例如搜尋器）有關資料當事人所提出關於刪除有關資料的連結或提供複本的要求¹¹²。

《通用數據保障條例》明確列明需要保留資料的例外情況：

- 為行使表達及資訊自由的權利；
- 為遵從法律責任，或為公眾利益或憑職權而執行的任務；
- 為公眾利益（例如公共健康範疇、管理健康或社會福利系統及服務等）；
- 為存檔、科學或歷史研究或公眾利益的統計用途；或
- 為確立、行使或維護法律申索¹¹³。

《〈通用數據保障條例〉下有關搜尋引擎的被遺忘權準則的第5/2019號指引（第1部）—公眾諮詢版本》¹¹⁴闡釋了要求搜尋引擎提供者除去連結（**除去資料要求**）的刪除權。該指引解釋資料當事人提出除去資料要求可援引的理據及需要保留資料的例外情況。該指引指出即使除去資料要求是根據確實理據作出，亦不會導致從源頭網站完全刪除有關個人資料，只會在以資料當事人的姓名作出搜尋時，從有關搜尋引擎結果中刪除特定的資料。

110 《私隱條例》第8部分述明保障資料原則的特定豁免，包括收集、使用及查閱

111 《通用數據保障條例》第17條

112 《通用數據保障條例》第17(2)條

113 《通用數據保障條例》第17(3)條

114 歐洲資料保障委員會於2019年12月2日採納作公眾諮詢

基於互聯網及搜尋引擎的環球性質，產生了被遺忘權的地域範圍及除去資料要求的適用程度問題。這個問題在歐洲法院的一宗案件中被提出。該案是關於Google與法國監管機構的爭議：搜尋引擎公司是否須把除去資料要求應用到其所有搜尋引擎的域名後綴，包括那些為歐盟以外用戶提供服務的搜尋引擎版本¹¹⁵。歐洲法院裁定營運者只須為歐盟成員國服務的搜尋引擎版本進行除去資料。不過，該營運者應防止或勸阻歐盟成員國的用戶透過其他網域查閱已除去的連結。

在香港，有關刪除資料的規定可見於《私隱條例》附表1的保障資料第2(2)原則及第26條。一般來說，資料使用者有責任採取所有切實可行的步驟，刪除不再需要用於原本收集目的（包括任何直接有關的目的）的個人資料。違反第26條會構成罪行，最高可被判處罰款一萬港元，但有例外情況，如有關刪除是受法律所禁止或刪除有關資料是違反公眾利益。

c. 提升反對處理的權利

在《通用數據保障條例》下，個人有權隨時反對根據下述基礎處理其個人資料¹¹⁶：

- (a) 為公眾利益而執行的任務或行使賦予資料控制者的職權；
- (b) 資料控制者或第三方追尋的合法利益；
- (c) 直接促銷目的；或
- (d) 科學或歷史研究目的或統計目的。

處理是包括個人概況彙編。《通用數據保障條例》第4(4)條對「**個人概況彙編**」所作的定義是「指以任何形式自動化地處理個人資料，以評估一名自然人的某些個人範疇，尤其是分析或預測該人的工作表現、經濟狀況、健康情況、個人喜好、興趣、可靠程度、行為、位置或動態」。

個人概況彙編的例子：

- ✓ 分析某人的互聯網瀏覽記錄及購物記錄，得出其偏好、興趣及習慣
- ✓ 有關某人的信貸申請分析或預測，當中並不涉及人為干預

¹¹⁵ Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés(CNIL), Case C-507/17

¹¹⁶ 《通用數據保障條例》第21條；其他處理資料的基礎（例如資料當事人同意、為履行合約所必需）載於《通用數據保障條例》第6條

資料控制者在收到反對根據上述(a)及(b)基礎而作出的資料處理活動之後，必須停止處理相關個人資料（包括個人概況彙編），除非它能展示有力的法律基礎，足以凌駕該人的利益、權利及自由，又或是為確立、行使或維護法律申索，以此維持處理個人資料（包括個人概況彙編）¹¹⁷。

有關根據上述(d)基礎（即科學或歷史研究目的或統計目的）而作出的個人資料處理，相關個人可依據其特別的情況而提出反對，除非有關處理是為公眾利益而進行的任務所必需的¹¹⁸。不過，純粹為直接促銷目的而處理個人資料（上述(c)基礎），則沒有例外情況可適用¹¹⁹。

根據《私隱條例》，一名個人在香港一般無權要求機構或企業停止「處理」¹²⁰其個人資料，但機構或企業在使用某人的個人資料作直接促銷用途前，須通知該人及取得其同意。此外，根據《私隱條例》第6A部，個人有權拒絕機構或企業使用或提供其個人資料以作直接促銷之用。

d. 新增限制處理的權利

根據《通用數據保障條例》，在下述情況下，個人有權限制資料控制者處理其個人資料，而資料控制者只可在過渡期儲存有關資料¹²¹，如：

- 個人質疑其個人資料的準確性，資料控制者須在一段時間內限制資料處理，以便核實其準確性；
- 有關資料處理是不合法的，但該人反對刪除個人資料，而只要求限制使用；
- 不再需要把個人資料用於相關處理，但該人仍需要用作確立、行使或維護法律申索；及
- 該人反對在核實控制者是否有合法理據可凌駕其權利的期間，繼續處理其個人資料。

在回應改正資料的要求時，根據《私隱條例》，香港的機構或企業若曾在過往的12個月內向第三方提供不準確的資料，但卻沒有理由相信該第三方已停止使用有關資料，則須採取合理切實可行的步驟通知該第三方¹²²。

117 《通用數據保障條例》第21(1)條及敘文69

118 《通用數據保障條例》第21(6)條

119 《通用數據保障條例》第21(2)條

120 根據《通用數據保障條例》第6(1)(a), 4(2), 4(11), 7, 8條及敘文43及32，「處理」涵蓋廣闊意義，包括收集、使用、披露、儲存、結集及刪除個人資料，視乎情況而定。可再參考上文關於《通用數據保障條例》的域外應用的部分。

121 《通用數據保障條例》第18條

122 《私隱條例》保障資料第2(1)(b)(i)原則

e. 新增權利：資料可攜權

這項新增權利可讓個人從一名資料控制者取得其個人資料的複本（須為具結構性、常用及機器可讀的格式），然後傳送予另一名資料控制者，條件是：

- 資料處理是按該個人的同意或履行合約作為法律基礎；及
- 資料處理是以自動化方式進行¹²³。

這項權利只限於個人已向資料控制者提供的個人資料。正如《資料可攜權利指引》¹²⁴ 闡述，這項新增權利旨在方便個人把一名資料控制者所持有關於他們的個人資料轉移、複製或傳送至另一名資料控制者。儘管如此，該兩名資料控制者並無責任將兩者在技術上不相容的系統變為相容¹²⁵。

在香港，《私隱條例》沒有訂明類似關於處理個人資料的限制或賦予資料可攜權。不過，機構及企業須依從個人所提出有關查閱及更正其個人資料的要求¹²⁶。

123 《通用數據保障條例》第20條

124 由歐盟第29條資料保障工作小組於2016年12月發出

125 《通用數據保障條例》敘文68

126 《私隱條例》第5部及附表1保障資料第6原則

資料保障印章、行為守則及司法管轄區之間的資料轉移

a. 認證 / 印章及行為守則

認證 / 印章

《通用數據保障條例》要求監管機構、歐洲資料保障委員會及歐盟委員會鼓勵建立資料保障認證機制、資料保障印章及標誌，讓資料控制者及資料處理者顯示其循規守法¹²⁷。認證制度可能尤其適用於從事雲端運算或多層資料處理的機構及企業，因個別審核或特定的資料保障合約條款未必適用。

發出的認證為期最多三年，視乎是否符合相關條件或規定可予續期或予以撤銷¹²⁸。認證可由私營或公營認證機構發出，而相關認證準則須由監管機構或歐洲資料保障委員會依據《通用數據保障條例》而核准。如準則是經由委員會核准，可成為共通的認證準則，即歐洲資料保障印章標誌¹²⁹。

認證屬自願性質。認證過程應具透明度。有關認證機制的資訊會備存於公共登記冊內。

認證不會減低資料控制者或資料處理者遵從《通用數據保障條例》的責任，亦不會損害監管機構的工作及權力。

歐洲資料保障委員會於2019年6月發出《認證及識別認證準則指引》¹³⁰。但截至2020年4月底，尚未有根據《通用數據保障條例》設立的認證機制。2019年12月，英國資訊專員公署宣佈會與英國皇家認證委員會制定認證計劃。

行為守則

《通用數據保障條例》亦鼓勵個別行業組織或團體因應其不同的資料處理的特質及中小微企業的需要，制定其業界專屬的行為守則¹³¹，歐盟成員國的監管機構會就有關行為守則是否符合《通用數據保障條例》規定作出核准或提供意見。但截至2020年4月底，尚未有根據《通用數據保障條例》核准的行為守則。

在香港，《私隱條例》第3部亦訂明，私隱專員在諮詢相關團體的代表及有利害關係的人士後，可核准實務守則¹³²。

127 《通用數據保障條例》第42(1)條

128 《通用數據保障條例》第42(7)條

129 《通用數據保障條例》第42(5)條

130 歐洲資料保障委員會於2019年6月4日採納有關根據條例第42及43條的認證及識別認證準則的第1/2018號指引

131 《通用數據保障條例》第40條

132 《私隱條例》第12條

b. 司法管轄區之間的資料轉移

轉移至歐盟以外的第三國或國際機構的個人資料仍然受到《通用數據保障條例》所規管¹³³。如接收資料國家或國際機構已取得歐盟委員會所作出的資料保障足夠度¹³⁴的評估決定¹³⁵，或有關轉移是有「適當的資料保障措施」¹³⁶，則有關轉移是獲准許的。歐盟指令在這方面的原有規定，大部分在《通用數據保障條例》獲得保留。

《通用數據保障條例》亦提供了詳盡的準則，以考慮非歐盟國家或國際機構是否可確保被轉移的個人資料獲得足夠的保障¹³⁷。歐洲資料保障委員會須向歐盟委員會提供意見，以評估某個國家或國際機構的保障程度是否足夠¹³⁸。截至2020年4月底，歐盟委員會已向13個司法管轄區¹³⁹發出資料保障足夠度的評估決定。但除了日本，對其餘12個司法管轄區的決定是根據歐盟指令而不是《通用數據保障條例》作出的。

在歐盟委員會尚未作出資料保障足夠度的評估決定時，跨司法管轄區轉移資料可援引的機制或安全措施包括採用歐盟核准的標準合約條款及企業約束規則，以及批准的認證或行為守則，加上由位處於第三國的資料控制者／資料處理者就施行這些適當的資料保障措施作出具約束力及可執行的承諾¹⁴⁰。

在香港，《私隱條例》第33條禁止轉移個人資料至香港境外，除非符合某些條件，例如目的地有足夠的措施保障轉移的資料。第33條尚未實施。該條沒有明確提及以認證或行為守則作為跨境資料轉移的足夠保障措施。

133 《通用數據保障條例》第V部

134 資料保障足夠度的評估決定是指歐盟委員會作出的一個決定，確認一個第三方國家、區域或一個或多於一個屬該第三方國家的界別，或所涉的國際機構達至足夠程度的保障（《通用數據保障條例》第45(1)條）

135 《通用數據保障條例》第45條

136 《通用數據保障條例》第46條

137 《通用數據保障條例》第45條

138 《通用數據保障條例》第45(2)條

139 該13個司法管轄區是安道爾、阿根廷、加拿大（商業機構）、法羅群島、根西島、以色列、馬恩島、日本、澤西、新西蘭、瑞士、烏拉圭及美國（限於私隱盾框架）。截至2020年4月底，正與南韓進行有關資料保障足夠度的討論。

140 《通用數據保障條例》第46及47條

懲罰

《通用數據保障條例》第58(2)(i)條賦權歐盟的監管機構對資料控制者及資料處理者實施兩級制的行政罰款。

依據《通用數據保障條例》第83(4)條，就違反下述規定者處以較低級別的行政罰款（即最高一千萬歐元，或上一個財政年度的全球年度總營業額的2%，以較高者為準）（非詳盡無遺）¹⁴¹：

- (a) 就處理兒童的個人資料取得家長的同意；
- (b) 如無必要識別資料當事人，以匿名方式處理個人資料；
- (c) 作出資料外洩事故通報；
- (d) 進行資料保障影響評估；及
- (e) 委任保障資料主任。

依據《通用數據保障條例》第83(5)條，就違反下述規定者處以較高級別的行政罰款（即最高二千萬歐元，或上一個財政年度全球年度總營業額的4%，以較高者為準）（非詳盡無遺）¹⁴²：

- (a) 遵從資料處理的基本原則，例如以合法、公平及具透明度的方式處理個人資料；
- (b) 以合法基礎處理個人資料，例如有效的同意；
- (c) 遵從資料當事人的權利，例如通知權、查閱個人資料權、修訂個人資料權、刪除權（被遺忘權）、反對處理的權利、反對自動化決策（包括個人概況彙編）的權利；及
- (d) 依據合法機制把個人資料轉移至第三國的接收者或國際機構。

大部分的歐盟監管機構在《通用數據保障條例》實施的首兩年都曾行使其行政罰款的權力。大多數罰款與違反下述規定有關：

- 有關處理個人資料的原則（第5條）；
- 資料處理的合法性（第6條）；
- 同意的條件（第7條）；
- 處理敏感個人資料（第9條）；
- 透明度與資料當事人的權利（第12至22條）；及
- 資料處理的保安及資料外洩事故（第32至34條）¹⁴³。

¹⁴¹ 見《通用數據保障條例》第8, 11, 33, 35及37條

¹⁴² 見《通用數據保障條例》第5-6, 13-22及44-49條

¹⁴³ 歐洲資料保障委員會於2020年2月18日採納的「歐洲資料保障委員會對《通用數據保障條例》第97條的評估」。

一些較矚目的行政罰款個案包括：

- 一個網上搜尋引擎在使用個人資料作個人化廣告時欠缺透明度及有效的同意，被法國監管機構判罰5,000萬歐元¹⁴⁴。該網上搜尋引擎在個人化廣告方面所提供的資訊不清晰、不全面，個別用戶不能容易查閱。此外，顯示用戶同意的格子是預先加上別號。
- 一間電訊公司非法處理個人資料作推廣用途，影響數以百萬人士，被意大利監管機構判罰2,780萬歐元。違規情況包括沒有有效同意而作出推廣電話，以及在管理有關個人資料方面欠缺問責性¹⁴⁵。
- 一間地產公司不必要地保留租戶的個人資料，被德國柏林監管機構判罰1,450萬歐元。該公司被監管機構警告後仍沒有採取適當行動，清理其資料庫，沒有貫徹資料保障的設計及預設¹⁴⁶。

其他正在處理中的行政罰款個案包括英國資訊專員公署擬對一間航空公司及一個酒店集團的資料外洩事故分別判罰1億8,300萬及9,900萬英鎊¹⁴⁷。

雖然《通用數據保障條例》第83(2)條列明決定行政罰款額的因素，但即使是類似的違規情況，不同的監管機構所判處的罰款亦差別甚大。歐洲資料保障委員會有可能就行政罰款制定歐盟適用的指引。目前，德國及荷蘭的監管機構已各自制定其指引。

在香港，如機構或企業違反《私隱條例》的規定（包括附表1的保障資料原則），私隱專員可依據《私隱條例》第50條向該機構或企業發出執行通知，指令它作出補救措施及（如適合的話）採取步驟防止違規事件再發生。不依從執行通知屬於犯罪¹⁴⁸。《私隱條例》為了處理一些嚴重的違規情況亦包含其他刑事罪行，例如《私隱條例》第6A部規管直接促銷活動的條文。刑事罪行的罰則是由香港的法院作出判定，私隱專員目前無權施加行政罰款。

144 歐洲資料保障委員會於2019年1月21日刊登的新聞，https://edpb.europa.eu/news/national-news_en

145 歐洲資料保障委員會於2020年2月1日刊登的新聞，https://edpb.europa.eu/news/national-news_en

146 歐洲資料保障委員會於2019年11月5日刊登的新聞，https://edpb.europa.eu/news/national-news_en

147 2019年7月，英國資訊專員公署公佈已發出了兩份意向通知書，分別向一個酒店集團判罰9,900萬英鎊及一間航空公司判罰1億8,300萬英鎊。該酒店集團於2018年11月通知資訊專員公署發生網絡事故，全球約3億3,900萬項客戶記錄受影響。該航空公司於2018年9月通知資訊專員公署發生網絡事故，約50萬名顧客的個人資料受影響。截至2020年5月底，這兩宗罰款尚未敲定。

148 《私隱條例》第50A條

更多有關 《通用數據保障條例》 的資訊

歐洲資料保障委員會是按《通用數據保障條例》成立的獨立歐盟機構，旨在促進執法方面的一致性和合作。該委員會亦就遵從《通用數據保障條例》的規定發出指引。委員會成員包括歐盟成員國國家監管機構的代表及歐洲資料保障監督。

要了解更多遵從《通用數據保障條例》的資訊，機構及企業可參考歐盟委員會的網站(http://ec.europa.eu/justice/data-protection/index_en.htm)及歐洲資料保障委員會的網站(https://edpb.europa.eu/edpb_en)。



香港個人資料私隱專員公署的網頁(www.pcpd.org.hk)內設有關於《通用數據保障條例》的專頁，並會適時更新資訊。

歐盟的《通用數據保障條例》及香港的《個人資料（私隱）條例》（主要分別）

	歐盟	香港
應用 	資料處理者或控制者： <ul style="list-style-type: none"> • 在歐盟設立公司，或 • 在歐盟以外設立公司，提供貨品或服務，或監察歐盟人士的行為。[第3條] 	資料使用者（控制者 / 處理者），獨自或聯同其他人或與其他人共同控制個人資料在香港或由香港收集、持有、處理或使用個人資料。[第2(1)條]
個人資料 	「個人資料」為： <ul style="list-style-type: none"> • 任何有關一名已被識別或可被識別的自然的資訊；而一名可被識別的自然人是指可直接或間接地被識別的。 • 可被明確地識別身份的個人資料的例子延伸至包括位置資料及網上識別符。[第4(1)條] 	「個人資料」為指符合以下說明的任何資料： <ul style="list-style-type: none"> • 直接或間接與一名在世的個人有關的； • 從該資料直接或間接地確定有關的個人的身分是切實可行的；及 • 該資料的存在形式令予以查閱及處理均是切實可行的。[第2(1)條]
問責與管治 	以風險為本；資料控制者須： <ul style="list-style-type: none"> • 實施技術性及機構性措施以確保循規 [第24條]； • 採取預設貫徹私隱的設計及預設 [第25條]； • 為高風險的處理活動進行資料保障評估 [第35條]；及 • （若屬某些類型的機構）委任保障資料主任。[第37條] 	沒有明確列明問責原則及相關的私隱管理措施。 私隱專員倡議採納私隱管理系統以顯示問責原則。委任保障資料主任及進行私隱影響評估是為達致問責而建議的良好行事方式。
敏感個人資料 	敏感個人資料的類別被擴大。 只在特定情況下才容許處理敏感個人資料。[第9條]	沒有以任何目的區分敏感及非敏感個人資料。

歐盟的《通用數據保障條例》及香港的《個人資料（私隱）條例》（主要分別）

	歐盟	香港
同意 	<p>同意必須是</p> <ul style="list-style-type: none"> • 自願給予、具體及知情； • 以聲明或清晰明確的行動不含糊地指明資料當事人的意願，表示同意處理其個人資料 [第4(1)條]；及 • 由16歲（或 13歲）以下兒童給予的同意須有家長授權。 	<p>同意不是收集個人資料的先決條件，除非個人資料是用於新目的。[保障資料第1及3原則] 在其他情況，若須徵求同意，同意是指自願作出的明示同意。</p> <p>沒有規定需要家長同意。</p>
通報資料外洩事故 	<p>資料控制者須向監管機構通報資料外洩事故，不可不當地延誤（例外情況適用）。</p> <p>如事故很可能對資料當事人的權利及利益造成高度風險，資料控制者須通知受影響的資料當事人，除非例外情況適用。[第33-34條]</p>	<p>沒有強制性規定，但考慮到所有持份者包括資料使用者 / 控制者 / 當事人的利益，應通報私隱專員（及資料當事人，如適用）。</p>
資料處理者 	<p>資料處理者負上額外責任以保存處理記錄、確保處理安全、通報資料外洩事故、委任保障資料主任等。[第30, 32-33, 37條]</p>	<p>資料處理者不是直接受規管。[第2(12)條]</p> <p>資料使用者須採取合約或其他方式以確保資料處理者循規。[保障資料第2(3)及4(2)原則]</p>
資料當事人新增或提升的權利 	<ul style="list-style-type: none"> • 就資料處理獲通知的權利 [第13-14條] • 刪除個人資料權（「被遺忘權」） [第17條] • 限制處理及資料可攜權 [第18及20條] • 反對處理（包括個人概況彙編）的權利 [第21條] 	<ul style="list-style-type: none"> • 對資料使用者 / 控制者就通知的要求相對未有如此廣泛 • 沒有刪除權，但資料不得保留超過所需的時間 [第26條及保障資料第2(2)原則] • 就資料處理沒有限制及沒有資料可攜權，但需遵從查閱資料及改正資料的權利 [保障資料第6原則，第5部] • 沒有反對處理資料的權利（包括個人概況彙編），但可拒絕直銷活動 [第35G及35L條]，而《私隱條例》中亦有條文規管資料核對程序 [第30-31條]

	歐盟	香港
<p>認證、印章、及行為守則</p> 	<p>設有明確認可機制以證明資料控制者及處理者合規。[第42條]</p>	<p>沒有正式的認證或私隱印章機制以證明合規。私隱專員在諮詢後可核准實務守則。[第12條]</p>
<p>司法管轄區之間的資料轉移</p> 	<p>述明認證及依從核准的行為守則作為其中一項資料轉移的法律基礎。[第46條]</p>	<p>認證制度及依從實務守則未有明確定為法律基礎。</p>
<p>懲罰</p> 	<p>監管機構獲授權可判處資料控制者及處理者行政罰款。[第58條]</p> <p>視乎違規的性質，罰款可達二千萬歐元或全球年度總營業額的4%。[第83條]</p>	<p>私隱專員沒有獲賦權施加行政罰款或刑罰。</p> <p>私隱專員可向資料使用者送達執行通知，在完成司法程序後違法者可能被判罰。[第50條]</p>

CONTENTS

Foreword	43
Why is the GDPR Relevant to Hong Kong Organisations and Businesses?	47
Extra-territorial Application of the GDPR	48
Personal Data Covered by the GDPR	54
New Data Privacy Governance, Data Mapping and Impact Assessment	56
a. Data Protection Officer	56
b. Data Protection Impact Assessment	59
c. Privacy by Design and by Default	61
d. Data Mapping	63
Sensitive Personal Data	64
Consent	67
a. Meaning of Consent	67
b. Digital Consent for Minors	70
Provision of Online Services and Use of Cookies	71
Mandatory Breach Notification	74
Data Processors' Obligations	76
New and Enhanced Rights for Individuals	80
a. Enhanced Right to Notice on Data Processing	80
b. Enhanced Right to Erasure ("Right to be Forgotten")	81
c. Enhanced Right to Object to Processing	83
d. New Right to Restriction of Processing	84
e. New Right to Data Portability	85
Data Protection Seals, Codes of Conduct and Cross-jurisdiction Data Transfer	86
a. Certification / Seals and Codes of Conduct	86
b. Cross-jurisdiction Data Transfer	87
Sanctions	89
More Information on the GDPR	92
EU GDPR and HK PDPO (Major Differences)	93

Foreword

The European Union (**EU**) has been spearheading the setting of personal data protection standard for more than two decades. The Data Protection Directive 1995 of the EU (**EU Directive**¹) was a benchmark legislation being followed or referenced by various jurisdictions, including Hong Kong. The General Data Protection Regulation 2016 (**GDPR**) of the EU² has set a new high-water mark when it became effective in all Member States of the EU and European Economic Area (**EEA**³) on 25 May 2018. Notable reforms brought by the GDPR include new and enhanced rights of individuals, accountability requirements on data controllers, sanctioning power of supervisory authorities and the extra-territorial application of the law. Given the close economic ties between Hong Kong and the EU, we published the first edition of this booklet in March 2018 to raise the awareness amongst all stakeholders in Hong Kong of the possible impact of the GDPR. This year marks the second anniversary of the GDPR implementation. We took stock of the implementation of the law and guidelines issued by European authorities to make this booklet more informative.

In the wake of technological developments and globalisation, the constitutionalisation of the fundamental right to data protection in the EU and the fragmentation of legislative 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;
- formulating a modern data protection framework; and
- governance based on accountability.

A recent report issued by the European Data Protection Board⁴ (**EDPB**) concluded that the implementation of the GDPR had been a success because it had "*strengthened data protection as a fundamental right*".⁵ The European Commission also remarked that since the implementation of the GDPR, "*citizens are becoming more aware of their rights*".⁶ Those views can be vindicated by the surge of data protection complaints in Europe in the last two years. For example, in the United Kingdom (**UK**), the Information Commissioner's Office received over 41,000 data protection complaints in 2018-19, which almost doubled the figure of the preceding fiscal year⁷. For the EU and EEA as a whole, over 275,000 data protection complaints were received by the

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

2 Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

3 The EEA comprises all EU Member States, Iceland, Liechtenstein and Norway.

4 EDPB is an independent EU body established by the GDPR to promote consistency and cooperation in the enforcement of the law. Members of the EDPB include representatives of the national supervisory authorities of the EU Member States and the European Data Protection Supervisor

5 EDPB, '*Contribution of the EDPB to the evaluation of the GDPR under Article 97*' adopted on 18 February 2020

6 Press release by the European Commission on 24 July 2019, 'General Data Protection Regulation shows results, but work needs to continue'

7 Annual Report 2018-19 of the Information Commissioner's Office of the UK

supervisory authorities during the period between 25 May 2018 and 30 November 2019. The number of complaints received by each supervisory authority varied considerably. Germany and the UK came top of the list with over 66,000 and 64,000 cases respectively during the first one-and-a-half years since the implementation of GDPR. The Netherlands came third with over 37,000 cases. Meanwhile, eight Member States received less than 1,000 cases each during the period⁸. The figures might reflect the differences in public attitudes towards and awareness of personal data protection in different Member States. We also received over 280 GDPR enquiries from the general public and a few GDPR-related complaints lodged by EU individuals against Hong Kong organisations over the last two years, despite the fact that we have no jurisdiction over those complaint cases. Hong Kong organisations and businesses with operations or businesses in Europe must remain vigilant about the heightened public expectation on data protection there.

From the compliance aspect, the European Commission noticed that "*Businesses are developing a compliance culture.*"⁹ Surveys also found that personal data protection had become one of the top priorities in many organisations and businesses. Organisations in the EU and many around the world, both large and small, have stepped up their efforts to ensure compliance with the GDPR. Personal data protection has become a board level issue and a business enabler, and has firmly linked to business strategies and goals. According to a study in May 2019, 500,000 organisations in the EU registered data protection officers under the GDPR¹⁰. The booming of the privacy management software market is another indicator of the change in corporate culture. The driving forces behind these changes include the elevated privacy expectation of consumers, accountability requirements under the GDPR and the strengthened penalties for GDPR violations.

On the enforcement front, EU supervisory authorities showed no hesitation in wielding their new formidable powers to impose administrative fines. According to the EDPB, between 25 May 2018 and 30 November 2019, 785 administrative fines were imposed by the supervisory authorities in 22 EU / EEA states¹¹. According to another unofficial study up to January 2020, a total of €114 million administrative fines were imposed by the supervisory authorities in 23 EU / EEA states, with France, Germany and Austria topping the rankings for the total values of fines¹². Reasons for imposing the fines were wide-ranging, including the lack of consent and transparency for processing of

8 EDPB, '*Contribution of the EDPB to the evaluation of the GDPR under Article 97*' adopted on 18 February 2020

9 Press release by the European Commission on 24 July 2019, 'General Data Protection Regulation shows results, but work needs to continue'

10 A study by the International Association of Privacy Professionals (IAPP)

11 EDPB, '*Contribution of the EDPB to the evaluation of the GDPR under Article 97*' adopted on 18 February 2020

12 DLA Piper GDPR data breach survey: January 2020. As of January 2020, those EU / EEA states which have imposed administrative fines under the GDPR are (in descending order in the value of total fines): France, Germany, Austria, Italy, Bulgaria, Spain, Poland, Greece, Netherlands, Portugal, Norway, Denmark, Romania, UK, Czech Republic, Hungary, Latvia, Cyprus, Slovakia, Lithuania, Sweden, Belgium and Malta; those EU / EEA states which have not imposed any fine under the GDPR are Croatia, Estonia, Finland, Iceland, Ireland, Liechtenstein, Luxemburg and Slovenia.

personal data, the lack of data security, retaining excessive amount of personal data, and even failing to notify supervisory authorities of the appointment of data protection officers.

Some commentators consider that so far the total number and amount of fines under the GDPR regime are not deterrent enough given that EU supervisory authorities have the power to fine up to 4% of total worldwide annual turnover of an organisation. That said, it would be unwise to assume that the infrequent and low-level fines are the norm. On the contrary, we should expect more fines will be imposed in future as the supervisory authorities have been staffing up their enforcement teams.

Apart from administrative fines, other regulatory powers in the toolboxes of EU supervisory authorities include issuing compliance orders and limiting (or even banning) the processing of personal data. Although the power of limiting or banning personal data processing is less frequently used (at least in reported cases), it is potentially more restrictive to an organisation or business, and hence should not be overlooked.

So far enforcement actions under the GDPR were mostly (if not all) taken against organisations and businesses with permanent establishments in the EU. Possible reasons include the limited resources of the supervisory authorities and the greater efforts needed to map out the mechanism for cross-jurisdiction enforcement. Nonetheless, Hong Kong organisations and businesses should not be lax in compliance if they fall within the jurisdiction of the law, even if they do not have a physical presence in the EU. With increased privacy awareness among EU individuals and the gradual staffing up in EU supervisory authorities, it would not be surprising that the regulators will soon test their extra-territorial powers. Hong Kong organisations and businesses should vigilantly assess whether their operations fall within the scope of the GDPR, and if "yes", whether they are compliant with the GDPR. After all, compliance with applicable laws is an obligation, as well as part and parcel of corporate governance.

The enactment of the GDPR also triggered a tsunami of legislative reforms around the world, including non-EU states (such as Brazil, India, Malaysia, the US and Thailand) that introduced or proposed introducing data protection legislation with similar requirements. In the mainland of China, the Personal Information Security Specification (a non-binding national standard on personal data protection) is widely considered as a regulatory response to the GDPR. In Hong Kong, we also made reference to the GDPR when reviewing the Personal Data (Privacy) Ordinance (Chapter 486 of the

Laws of Hong Kong) (**PDPO**). Convergence or defragmentation in data protection laws and standards on a global scale towards the higher water mark seems to be gathering momentum. Organisations and businesses operating in this increasingly connected world should strive to meet the highest data protection standard in order to ensure compliance with various regulatory frameworks and meet consumers' expectation. Regulation shopping is not a viable option in the long run.

Despite the fact that the GDPR has been effective for two years and a number of guidelines have been issued, some teething problems persist. A few major provisions of the law need further guidance and clarifications. Examples include the threshold for making data breach notifications to supervisory authorities under Article 33, certification mechanisms of data processing activities under Article 42 and assessment on the levels of administrative fines under Article 83. The threshold of data breach notification is reportedly ambiguous and arguably low. Compounded with the potentially heavy fines for failing to make notifications, many trivial and minor data breaches were reported to the supervisory authorities, draining their scarce resources. Certification is one of the highlights of the GDPR because it will enable demonstrating compliance and accountability, as well as cross-jurisdictional transfer of personal data. However, certification mechanism does not appear to have been established under the GDPR so far. The different levels of administrative fines imposed by different supervisory authorities for similar violations also give rise to some concerns on consistency and fairness. In 2019, the German and Dutch supervisory authorities issued their own guidelines for calculating administrative fines with a view to increasing the predictability of fines. However, EU-wide guidelines to standardise the level of fines are not yet available.

By updating this booklet, we aim to provide more comprehensive and up to date information on the GDPR. However, this booklet is 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 official sources, i.e. the European Commission, EDPB and EU supervisory authorities. Organisations and businesses should seek specific legal advice to prepare themselves for the appropriate changes in their privacy policies, practices and procedures where appropriate.

Stephen Kai-yi WONG
Privacy Commissioner for Personal Data, Hong Kong
May 2020

Why is the GDPR Relevant to Hong Kong Organisations and 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 1980¹³ and the EU Directive. In consequence, the PDPO and the EU Directive 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 and businesses in Hong Kong to ascertain if the GDPR is applicable to them, and hence be complied with.

¹³ *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

An organisation or 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 (**Establishment Criterion**); 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 (**Targeting Criterion**)¹⁴.

The *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)*¹⁵ suggests that the territorial scope of the GDPR is on the basis of the two main criteria mentioned above: the Establishment Criterion and the Targeting Criterion. It further highlights that Article 3 of the GDPR aims at determining whether a particular processing activity, rather than a person (legal or natural), falls within the scope of the GDPR. Hence, certain data processing activities of a Hong Kong organisation / business might fall within the scope of the GDPR, while other data processing activities of this same organisation / business might not.

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.

Establishment Criterion

An organisation or 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 EU¹⁶. However, a data processor¹⁷ in the EU should not be considered to be an establishment of a data controller merely by virtue as processor on behalf of the controller¹⁸.

¹⁴ Article 3 of the GDPR

¹⁵ Adopted by the EDPB on 12 November 2019

¹⁶ *Weltimmo v. NAIH*, Case C-230/14

¹⁷ A data processor means a person or an entity which processes personal data on behalf of a data controller

¹⁸ See *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)*

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

Generally, the GDPR may affect organisations and businesses established in the EU acting in the role of **data controllers** and **data processors**¹⁹ processing personal data in the context of that establishment, **regardless of whether the personal data is actually processed in the EU**²⁰.

It is not necessary that the processing in question is carried out by the relevant EU establishment itself. The question is whether there is **an extricable link between the processing in question and the activities of the EU establishment**²¹.

Example: An e-commerce website operated by a company based in the mainland of China, in which data processing activities are exclusively carried out in China, has established a European office in Berlin in order to lead and implement commercial prospection and marketing campaigns towards EU markets. The activities of the European office in Berlin are inextricably linked to the processing of personal data carried out by the Chinese e-commerce website.

The processing of personal data by the Chinese company can therefore be regarded as carried out in the context of the activities of the European office, as an establishment in the EU, and therefore be subject to the provisions of the GDPR.

(adopted from the Guidelines 3/2018 on the territorial scope of the GDPR (Article 3))

19 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.

20 See Article 29 Data Protection Working Party (WP29)'s EU General Data Protection Regulation: General Information Document

21 See Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)

Under the Establishment Criterion, the application of the GDPR is not restricted to the processing of personal data of individuals who are in the EU.

Example: A French company has developed a car-sharing application exclusively addressed to customers in Morocco, Algeria and Tunisia. The service is only available in those three countries but all personal data processing activities are carried out by the data controller in France.

While the collection of personal data takes place in non-EU countries, the subsequent processing of personal data in this case is carried out in the context of the activities of an establishment of a data controller in the EU. Therefore, even though processing relates to personal data of data subjects who are not in the EU, the GDPR will be applicable to the processing carried out by the French company.

(adopted from the Guidelines 3/2018 on the territorial scope of the GDPR (Article 3))

Targeting Criterion

The GDPR may also affect Hong Kong organisations and 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 or 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)

The application of this criterion is not limited by the citizenship, residence or other type of legal status of the individuals whose personal data are being processed. It is the location of the individuals that is the determining factor²².

Example: A bank in Taiwan has customers who are residing in Taiwan but holding German citizenship. The bank is active only in Taiwan. Its activities are not directed at the EU market.

The bank's processing of the personal data of its German customers is not subject to the GDPR.

(adopted from the Guidelines 3/2018 on the territorial scope of the GDPR (Article 3))

However, the fact of processing personal data of an individual in the EU alone is not sufficient to trigger the application of the GDPR to processing activities of an organisation or business not established in the EU. The element of "targeting" individuals in the EU, either by offering goods or services to them or by monitoring their behaviour, must always be present in addition²³.

Example: A U.S. citizen is travelling through Europe during his holidays. While in Europe, he downloads and uses a new app that is offered by a U.S. company. The app is exclusively directed at the U.S. market.

The collection of the U.S. tourist's personal data via the app by the U.S. company is not subject to the GDPR.

²² See *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)*

²³ See *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)*

Example: A Swiss University is launching its Master degree selection process, by making available an online platform where candidates can upload their CV and cover letter, together with their contact details. The selection process is open to any student with a sufficient level of German and English and holding a Bachelor degree. The University does not specifically advertise to students in EU Universities, and only takes payment in Swiss currency.

As there is no distinction or specification for students from the EU in the application and selection process for this Master degree, it cannot be established that the Swiss University has the intention to target students from a particular EU Member State. The sufficient level of German and English is a general requirement that applies to any applicant whether a Swiss resident, a person in the EU or a student from a third country. Without other factors indicating the specific targeting of students in EU Member States, it therefore cannot be established that the processing in question relates to the offer of education service to data subjects in the EU, and such processing will therefore not be subject to the GDPR.

(both adopted from the Guidelines 3/2018 on the territorial scope of the GDPR (Article 3))

Designation of Representative

Organisations and businesses meeting the Target Criterion are required to designate a representative in the EU unless an exemption applies²⁴.

The representative shall, on behalf of the organisation or business, cooperate with the competent supervisory authorities and communicate with data subjects. It may be a natural or legal person and should be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are located. As part of the transparency obligations, the organisation or business should provide data subjects with information as to the identity of their representative in the EU²⁵.

Example: A website, based and managed in Turkey, offers services for the creation, edition, printing and shipping of personalised family photo albums. The website is available in English, French, Dutch and German and payments can be made in Euros or Sterling. The website indicates that photo albums can only be delivered by post mail in France, Benelux countries and Germany.

This website is subject to the GDPR and the data controller must designate a representative in one of the Member States where the service offered is available, in this case either in France, Belgium, Netherlands, Luxembourg or Germany.

(adopted from the Guidelines 3/2018 on the territorial scope of the GDPR (Article 3))

²⁴ Article 27 of the GDPR

²⁵ See *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)*

Personal Data Covered by the GDPR

The GDPR protects "personal data", which is defined as "*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*"²⁶.

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)).

If an individual can be distinguished (or singled out) from other individuals, then that individual is "identified" or is "identifiable". For example, an individual's username on social media is personal data if it distinguishes the individual from others, regardless of whether it is possible to link the 'online' identity with a 'real world' named individual²⁷.

In determining whether a natural person is identifiable, the GDPR states that account should be taken of all the means reasonably likely to be used²⁸. To ascertain whether means are "*reasonably likely to be used*", all objective factors should be taken into account, such as the costs and the amount of time required for identification and the available technology²⁹.

In a case based on the EU Directive of 1995, the Court of Justice of the EU held that a dynamic IP address recorded by a website operator (in this case a German governmental body) when an individual visits the website constitutes personal data of that individual, provided that the website operator has legal means to identify the individual with the additional information in the possession of the internet service provider³⁰. The Court's decision will likely continue to apply to GDPR-related cases because the definition of personal data under the GDPR is similar to and wider than that under the EU Directive of 1995.

26 Article 4(1) of the GDPR

27 See *Guide to the General Data Protection Regulation (GDPR)* published by the Information Commissioner's Office of the UK, available at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>

28 Recital 26 of the GDPR

29 Recital 26 of the GDPR

30 *Patrick Breyer v Bundesrepublik Deutschland*, Case C-582/14

Personal data that has been de-identified, encrypted or pseudonymised but can be used to re-identify a person remains personal data and falls within the scope of the GDPR³¹.

Personal data that has been rendered anonymous in such a way that the individual is not identifiable anymore is no longer considered personal data. For data to be truly anonymised, the anonymisation must be irreversible³².

31 See "*What is personal data?*" published by the European Commission, available at https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

32 *Ditto*

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 activities³³.

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 GDPR³⁴;
- undertaking **Data Protection Impact Assessment (DPIA)** to identify and manage data protection risks³⁵;
- 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 safeguards³⁶;
- Keeping **records** of processing activities³⁷; and
- drawing up data processing or handling **policies or practices** to demonstrate compliance and accountability³⁸.

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 Officers³⁹ provide guidance on the designation of a DPO, the expertise and skills required.

33 Articles 5, 24 and 25 of the GDPR

34 Article 37 of the GDPR (for the applicable types of organisations / businesses)

35 Article 35 of the GDPR

36 Article 25(1) of the GDPR

37 Article 30 of the GDPR

38 Article 24(2) of the GDPR

39 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 situations⁴⁰:

- it is a public authority or body (with minor exemptions for courts acting in a judicial capacity);
- its core activities⁴¹ consist of processing operations which require regular and systematic monitoring⁴² of data subjects on a large scale⁴³; 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.

It is estimated that 500,000 organisations have registered DPOs across the EU within the 1st year implementation of the GDPR⁴⁴.

The DPO shall perform at least the following tasks⁴⁵:

- 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.

40 Article 37(1) of the GDPR

41 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*).

42 Classic example of "regular and systematic monitoring" will include activities such as online tracking, profiling, credit scoring, etc.

43 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.

44 According to a study conducted by the International Association of Privacy Professionals (IAPP)

45 Article 39(1) of the GDPR

In December 2019, a German subsidiary of a social media platform was fined by the Hamburg Commissioner for Data Protection and Freedom of Information for €51,000 for failing to notify the supervisory authority of the appointment of a new DPO, which was in contravention of Article 37(7) of the GDPR. While the amount of fine is not considered substantial, it serves as a warning to the controllers that appointing a DPO and reporting to the supervisory authority about the appointment and duties of the DPO are data controllers' obligations that should not be disregarded. The social media platform did not appeal against the fine and made payment correspondingly.

In December 2019, Germany's Federal Commissioner for Data Protection and Freedom of Information also issued a fine of €10,000 against a small telecommunications provider in Germany for its failure to appoint a DPO pursuant to Article 37(1) of the GDPR. The supervisory authority said the amount of the fine reflected the company's failure to comply with repeated requests, but the penalty was not considered substantial because the company belonged to the category of micro-enterprises.

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 and businesses must provide sufficient resources for a DPO to carry out his task, and he should not be penalised or dismissed for performing his tasks⁴⁶. 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 data⁴⁷.

⁴⁶ See part 3 of the *EU WP29 Guidelines on Data Protection Officers*

⁴⁷ Article 38(6) of the GDPR

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 and businesses to adopt the Privacy Management Programme⁴⁸ (**PMP**) which manifests the accountability principle. The PMP serves as a strategic framework to assist an organisation or 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 organisations' or businesses' commitment to good corporate governance and building trust with their employees and customers through open and transparent information policies and practices. The appointment of a DPO is recommended as a good practice under the PMP.

b. Data Protection Impact Assessment

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

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 controller⁴⁹. In particular, DPIA is required when it involves⁵⁰:-

- 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.

48 See *Privacy Management Programme – A Best Practice Guide* issued by the PCPD, available at www.pcpd.org.hk/english/resources_centre/publications/files/PMP_guide_e.pdf

49 See *WP29 Guidelines on Data Protection Impact Assessment adopted on 4 October 2017*

50 Article 35 of the GDPR

Concrete examples of the types of conditions that would require carrying out of a DPIA include:

- an organisation using new technologies (such as facial recognition) to monitor or track people's location or behaviour systematically;
- a financial institution screening its customers against a credit reference database and making automated decisions about customers' loan applications;
- a hospital establishing and implementing a new health information database with patients' health data;
- the gathering of public social media data for generating profiles.

As a matter of good practice, a DPIA should be continuously reviewed and regularly re-assessed. Data users shall bear in mind that conducting a DPIA is a continuous process, not a one-time exercise.

Under the GDPR, failure to carry out a DPIA when required may attract a fine of up to €10 million, or 2% global annual turnover, whichever is higher.

The PCPD has published an *Information Leaflet on Privacy Impact Assessments*⁵¹ to guide organisations and 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 buildings⁵².

51 See PCPD's website: www.pcpd.org.hk/english/resources_centre/publications/files/InfoLeaflet_PIA_ENG_web.pdf

52 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

c. Privacy by Design and by Default

Organisations and 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 GDPR⁵³.

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;
- 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 accessibility⁵⁴.

On 13 November 2019, the EDPB published its draft *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*⁵⁵ to provide practical guidance and examples on how to implement data protection by design and by default in the context of the data protection principles. For example, in upholding the transparency principle, a privacy policy (which contains information about how a data controller collects, uses and shares personal data) shall be accessible to all, including the use of machine readable languages to facilitate and automate readability and clarity. The privacy policy should also be provided in different channels and media, beyond the textual, to increase the probability for the information to effectively reach the data subject. In terms of fairness, default options for personal data processing must be the least invasive, and the choice for further processing must be presented in a manner that does not deter the data subject from abstaining. If algorithms are deployed to analyse and make predictions about the data subjects, they shall be fully informed.

53 Article 25(1) of the GDPR

54 Article 25(2) of the GDPR

55 The public consultation of this draft guideline closed on 16 January 2020.

Penalties

On 30 October 2019, the Berlin Commissioner for Data Protection and Freedom of Information issued a €14.5 million fine on a German real estate company for (i) retaining tenants' personal data substantially longer than necessary and (ii) infringing the data protection by design requirement⁵⁶. During the on-site inspections in June 2017 and March 2019, the supervisory authority found that the company used an archive system for the storage of personal data of tenants that did not provide the possibility of removing data that was no longer required. Personal data of tenants (including bank statements, salary statements, extracts from employment and training contracts, tax, social security and health insurance data) was stored without checking whether storage was permissible or necessary. The fine is considered high because the supervisory authority took the view that the real estate company deliberately created the data archive in question and processed the data inappropriately over a long period of time.

An education agency was also fined by the Norwegian supervisory authority on 11 October 2019 for €120 000⁵⁷ for its poor security of processing personal data in a mobile app which was used for communication among school employees, parents and pupils. Special category personal data, such as health data of children was processed. The poor security of the app allowed unauthorised persons to access and alter personal data of more than 63,000 pupils. The supervisory authority found that this was a result of inadequate security testing before the app was launched. This case reminds organisations to build security testing time and budget into the development process and support security testing (which is the concept of privacy by design and by default). Security testing before launching an app is helpful in identifying and assessing the risk of the applications for unauthorised access such that adequate authentication controls can be implemented.

⁵⁶ As of March 2020, the decision has not yet become final as the real estate company has indicated that it would appeal against the decision.

⁵⁷ Originally, the supervisory authority imposed a fine of €200 000 in response to the breaches. However, the final amount was reduced to €120 000 as there were mitigating factors present including implementing measures to limit the damages promptly and showing willingness to resolve the issues.

d. Data Mapping

Organisations and 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.⁵⁸

Organisations and 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 activities⁵⁹.

Organisations and 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 it to be 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 and 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 and businesses in Hong Kong are required to make their privacy policies and practices transparent⁶⁰. It is also one of the key components of the PMP for data users to maintain a personal data inventory such that organisations and businesses can benefit from carefully examining the personal data they hold and how they currently handle the data.

58 For other details of the record, see Article 30(1) and (2) of the GDPR.

59 Article 30(5) of the GDPR

60 Data Protection Principle (DPP) 5 in Schedule 1 to the PDPO

Sensitive Personal Data

The GDPR imposes more stringent requirements than the EU Directive on the processing of special categories of personal data⁶¹. 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; (ii) where the processing is necessary for reasons of substantial public interest, which is proportionate to the aim pursued; or (iii) where the processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health, etc⁶².

The global outbreak of COVID-19 in March 2020 has raised privacy concerns over the use and processing of personal data in the context of the fight against the coronavirus across various jurisdictions in the EU. In the "Statement on the processing of personal data in the context of the COVID-19 outbreak" adopted by the EDPB on 19 March 2020, the EDPB recognised that there were derogations to the prohibition of processing of certain special categories of personal data, such as health data, where it would be necessary for reasons of substantial public interest in the area of public health⁶³, on the basis of EU or Member States' laws, or where there would be the need to protect the vital interests of the data subject⁶⁴, as Recital 46 of the GDPR explicitly refers to

61 Article 9 of the GDPR

62 For other conditions governing sensitive personal data, please refer to Article 9(2) of the GDPR.

63 Article 9(2)(i) of the GDPR

64 Article 9(2)(c) of the GDPR

the control of an epidemic. In the fight against the coronavirus pandemic, the EDPB reckoned that while data protection rules (such as the GDPR) should not hinder measures taken to fight the coronavirus, data controllers must ensure the protection of personal data privacy and guarantee lawful processing of personal data. Emergency would be a legal condition which might legitimise restrictions of freedoms provided that the restrictions were proportionate and limited to the emergency period.

Penalties relating to collection of sensitive personal data

On 20 August 2019, a high school in Sweden was fined SEK 200,000 (equivalent to around €18,630) by the Swedish supervisory authority for collecting students' facial images (which are regarded as sensitive data) for attendance record purpose. The supervisory authority opined that, given the significant imbalance of the relationship between the school board and the students, and the fact that attendance records were a one-side control measure, consent from the students or their parents could not be considered voluntary and used as a legal basis for exempting the prohibition to use sensitive personal data of students. Hence, Article 9 of the GDPR was violated. Apart from violating Article 9, the supervisory authority also ruled that the use of facial recognition technology was disproportionate to the purpose (i.e. registering attendance) and registering attendance in class could be made in less intrusive ways.

On 17 December 2019, the UK Information Commissioner's Office fined a London-based pharmacy £275,000 for failing to ensure the security of special category data, constituting an infringement of the GDPR. The pharmacy had left approximately 500,000 documents (containing names, addresses, dates of birth, NHS numbers, medical information and prescriptions) in unlocked containers on its premises.

In a related guideline adopted by the EDPB on processing personal data through video devices⁶⁵, the EDPB laid down some considerations for processing of special categories of data, such as a video surveillance system with facial recognition technology to uniquely identify a person. To start with, the data controller must identify both an exception for processing special categories of data under Article 9 of the GDPR (i.e. a derogation from the general rule that one should not process special categories of data) and a legal basis for the data processing under Article 6. The processing of biometric data by facial recognition technology entails heightened risks for data subjects' rights and would therefore require enhanced and continued vigilance with regard to certain obligations, such as a higher level of security and a data protection impact assessment, where necessary. The deployment of video surveillance including facial or other biometric recognition installed by businesses for their own commercial purposes will generally require the explicit consent of all individuals.

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 and businesses to take into account the type of personal data when considering the appropriate measures to be implemented to ensure the security of the data⁶⁶. Hence, safeguards or security measures should be commensurate with the sensitivity of the personal data. The PCPD has published the *Guidance on Collection and Use of Biometric Data*⁶⁷, providing guidance and recommended good practices to data users who collect and use biometric data, which is considered as sensitive data by nature of its uniqueness and intimacy to a data subject's health, mental condition or racial origin.

65 *Guidelines 3/2019 on processing of personal data through video devices* adopted by the EDPB on 29 January 2020

66 See DPP4 in Schedule 1 to the PDPO

67 See PCPD's website: https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_biometric_e.pdf

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 include⁶⁸:-

- consent of the data subject to the processing for one or more specific purposes;
- 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*⁶⁹. (emphasis added)

When obtaining consent from data subjects in the form of a written declaration, organisations and 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 language⁷⁰. Apart from basic information, such as the data controller's identity and the type of data to be collected and used, data subjects should also be informed of their right to withdraw their consent.

68 Article 6(1)(a) to (f) of the GDPR

69 Article 4(11) of the GDPR

70 Article 7 of the GDPR

Examples of valid and invalid consent:

- ✗ An individual is not allowed to give separate consent for different personal data processing operation
- ✗ Bundled consent situation where the performance of a service contract is made conditional on the consent given to such processing activities which are unnecessary
- ✗ Default setting to pre-tick a box to agree to the terms and conditions
- ✗ Silence and inaction of the data subject

- ✓ Ticking boxes when visiting a website to give consent for specific data processing purposes
- ✓ Choosing the technical settings for an app installed for smartphone
- ✓ Making it clear that refusal or withdrawal of consent would not lead to denial of service

The data controller must ensure that consent can be withdrawn as easy as giving consent and at any given time⁷¹. If an individual withdraws consent, the data controller must stop the relevant processing and cannot swap from consent to other lawful bases⁷². For more detailed clarification and specification of requirements for obtaining and demonstrating valid consent, please refer to the *Article 29 Working Party Guidelines on consent under Regulation 2016/679*⁷³.

71 Article 7(3) of the GDPR

72 See Part 6 of the *Article 29 Working Party Guidelines on consent under Regulation 2016/679*

73 Endorsed by the EDPB in May 2018

Since the GDPR came into operation, some data controllers have been held liable for processing personal data without valid consent, for example:

- A global online search engine company was fined €50 million by the French supervisory authority for failing to validly obtain consent of data subjects for its advertisement personalisation, e.g. using a pre-ticked box, obtaining a general consent to all its processing operations;
- An energy retail company was fined €8.5 million by the Italian supervisory authority for making advertising calls without consent and obtaining data of prospective customers from entities that had not obtained any consent for the disclosure of such data;
- The Greek supervisory authority imposed a fine of €150,000 upon a global accounting and auditing firm for processing its employees' personal data on an inappropriate basis of consent as consent of employees in general cannot be regarded as freely given due to the clear imbalance between the parties⁷⁴.

⁷⁴ See Part 3.1.1 of the Article 29 Working Party Guidelines on consent under Regulation 2016/679

b. Digital Consent for Minors

Organisations and 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"⁷⁵ (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 responsibility⁷⁶.

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 and 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 or for direct marketing. "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 and 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) minor⁷⁷, (ii) incapable of managing his own affairs, or (iii) mentally incapacitated, the PDPO allows the "relevant person"⁷⁸ 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 subject⁷⁹.

75 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."

76 Article 8 of the GDPR

77 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)).

78 "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).

79 DPP3(2) in Schedule 1 to the PDPO

Provision of Online Services and Use of Cookies

Online services have become an integral part of our daily lives and tracking of user behaviour is often carried out by online services providers for purposes such as target advertising and personalisation of content. Organisations and businesses with establishments in the EU or targeting at individuals in the EU should ensure that their websites process personal data in a fair and transparent manner, in line with the purpose limitation and data minimisation obligations, and on a lawful basis (e.g. consent of data subject, necessary for performance of contract etc.).

According to *the Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*⁸⁰, the concept of what is "necessary for the performance of a contract" under Article 6(1)(b) of the GDPR⁸¹ is not simply an assessment of what is permitted by or written into the terms of a contract. Data controllers should carry out a fact-based assessment of the data processing activity in question with the objective pursued and of whether it is less intrusive compared to other options for achieving the same objective.

Example: A data subject buys items from an online retailer. The data subject wants to pay by credit card and for the products to be delivered to his home address. In order to fulfil the contract, the retailer must process the data subject's credit card information and billing address for payment purposes and the data subject's home address for delivery. Thus, Article 6(1)(b) of the GDPR is applicable as a legal basis for these processing activities.

However, if the customer has opted for shipment to a pick-up point, the processing of the data subject's home address is no longer necessary for the performance of the purchase contract. Any processing of the data subject's address in this context will require a different legal basis.

(adopted from the Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects)

80 Adopted by the EDPB on 8 October 2019

81 The basis under Article 6(1)(b) of the GDPR is "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract".

Personalisation of content is not regarded as necessary for the performance of contract unless it constitutes an intrinsic and expected element of certain online services⁸². In such cases, data controllers should consider an alternative lawful basis where applicable.

Example: An online hotel search engine monitors past bookings of users in order to create a profile of their typical expenditure. This profile is subsequently used to recommend particular hotels to a user when returning search results. In this case, profiling of a user's past behaviour and financial data would not be objectively necessary for the performance of a contract, i.e. the provision of hospitality services based on particular search criteria provided by the user. Therefore, Article 6(1)(b) of the GDPR would not form an applicable basis for this processing activity.

(adopted from *the Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*)

Nowadays, organisations and businesses often use cookies, a small text file stored in computers or mobile devices, to track website users' online activities. Apart from first-party cookies used by a website operator directly, there are also third-party cookies that are often used by advertisers to build profiles of users and conduct targeted advertising. Online identifiers (such as IP addresses and cookie identifiers) may be used to create profiles of individuals and identify an individual⁸³. Hence, the use of cookies may constitute processing of personal data under the GDPR.

Supervisory authorities of the UK, France, Germany and Spain published their own guidance on the use of cookies and other internet-tracking technologies. For example, the Information Commissioner's Office of the UK highlights in the *Guidance on the use of cookies and similar technologies*⁸⁴ that an individual's continued use of the website does not constitute valid consent and a pre-ticked box cannot be used for non-essential cookies.

82 See Part 3 of the *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*

83 Recital 30 of the GDPR provides: "Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them."

84 Available at <https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf>

This view has been affirmed by the Court of Justice of the EU in October 2019 in a case concerning the use of cookies by a lottery website⁸⁵. Although the case is based on e-Privacy Directive⁸⁶ which seeks to particularise and complement the GDPR with respect to the processing of personal data in the electronic communication sector⁸⁷, the Court made reference to the concept of "consent" under the GDPR. It ruled that before website operators drop and access non-essential cookies such as marketing cookies, the user must have given specific consent by actively selecting to opt-in. A pre-checked box for user to de-select or opt-out in order to refuse consent is no longer sufficient.

Although there is no specific provision on online identifiers or electronic communication in the technology-neutral PDPO, the PCPD has published a number of information leaflets on privacy issues relating to information and communications technology for reference by members of the public, such as *Privacy Implications for Organisational Use of Social Networks*, *Online Behavioural Tracking*, *Personal Data Privacy Protection: What Mobile Apps Developers and their Clients should know*⁸⁸.

85 *Verbraucherzentrale Bundesverband e.V. v. Planet49 GmbH*, Case C-673/17

86 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) as amended by Directive 2006/24/EC and Directive 2009/136/EC

87 See EDPB's *Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities*

88 Available at PCPD's website at https://www.pcpd.org.hk/english/resources_centre/publications/information_leaflet/information_leaflet.html

Mandatory Breach Notification

Under the GDPR⁸⁹, it is mandatory for organisations and businesses to give data breach notification. They are required under the GDPR to notify 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 circumstances⁹⁰. The same obligation is imposed on organisations and businesses which are acting in the role of data processors.

The prescribed contents to be included in a data breach notification to the supervisory authority⁹¹:-

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

As suggested in the *Guidelines on Personal Data Breach Notification under Regulation 2016/679*⁹² and the *Guidelines on Personal Data Breach Notification for the European Union Institutions and Bodies*⁹³, the data breach notification obligation reflects a "risk-based approach" and severity of breaches shall be assessed on a case-by-case basis. When assessing whether there is a "*risk to the rights and freedom of individuals*", the following factors have to be considered:

- type of breach;
- nature, sensitivity, and volume of personal data;
- ease of identification of individuals;
- severity of consequences for individuals;
- special characteristics of the affected individuals;
- special characteristics of the data users; and
- the number of affected individuals.

89 Article 33

90 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.

91 Articles 33-34 and Recitals 85-86 of the GDPR

92 Issued by the WP29 and adopted on 6 February 2018

93 Issued by the European Data Protection Supervisor on 21 November 2018

Each of the factors above have to be carefully assessed separately or in combination with the others to indicate the level of the risks to the individuals.

Examples of personal data breaches which meet the threshold of notifying both the supervisory authority and the affected data subjects:

- ✓ Personal data of a large number of students are mistakenly sent to the wrong mailing list with 1000+ recipients
- ✓ Medical records in a hospital are unavailable for a period of 30 hours due to a cyber-attack
- ✓ A database containing information on whistleblowing procedures has been hacked and published on the internet. The names of whistle-blowers and persons concerned have been made public
- ✓ An agency suffers a ransomware attack that results in all personal data of citizens registered in a specific funding programme being encrypted. No back-ups are available and the data cannot be restored

In May 2019, a political party in Hungary was fined HUF11 million (€32,000) by the Hungarian National Authority for Data Protection and the Freedom of Information for failing to notify the supervisory authority and affected individuals of a data breach under Article 33(1) and Article 34(1) and failing to document the facts of the data breach, its effects and remedial actions taken under Article 33(5) of the GDPR. The breach was the result of a cyber-attack by a hacker who accessed the organisation's system and disclosed information (such as names, emails, and passwords) of more than 6,000 individuals.

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*⁹⁴, which explains the actions to be taken for giving notification. It is a recommended good practice for organisations and businesses to give notification to the PCPD and any affected individuals as soon as possible so as to ensure that actions will be taken without undue delay to mitigate any possible harm.

94 See PCPD's website: www.pcpd.org.hk/english/resources_centre/publications/files/DataBreachHandling2015_e.pdf

Data Processors' Obligations

Organisations and 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 subjects⁹⁵. In addition, contract 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 contracts⁹⁶ 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 the 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.

95 Article 28 of the GDPR

96 Article 28(3) of the GDPR

In December 2018, a small shipping company in Germany was fined €5,000 by the Hamburg Commissioner for Data Protection and Freedom of Information for its failure to enter into a processing contract with its service provider (being a data processor) under Article 28(3) of the GDPR to detail the security measures taken by the service provider, and how they complied with the GDPR standards. The absence of such a contract led the supervisory authority to conclude that sensitive data had been transmitted to the service provider without the proper legal bases in place. Another aggravating factor was that the practice had been going on for some time and steps had deliberately not been taken to rectify the procedures, despite the company being aware of its duties under the GDPR.

The GDPR also imposes direct obligations on data processors including (but not limited to)⁹⁷:-

- 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 the EU under prescribed conditions only.

⁹⁷ 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.

The GDPR includes a limited exception for organisations and businesses 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 enterprises⁹⁸ in the application of the GDPR.

Data Processors are regulated directly by supervisory authorities under the GDPR, and they are liable to be penalised for breach of their obligations (e.g. failure to report a data breach)⁹⁹. Direct regulation has prompted data processors to attain same level of diligence and caution as data users to data security, retention and use of personal data.

The applicability of the GDPR on a data processor established outside the EU is further clarified in the *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)*¹⁰⁰. To consider whether a non-EU processor is subject to GDPR, one has to look at whether the processing activities by the processor are related to activities of the controller that are targeted at individuals in the EU. Where processing activities by the controller relate to the offering of goods or services or to the monitoring of individuals' behavior in the EU (i.e. targeting), any processor instructed to carry out that processing activity on behalf of the controller will fall within the scope of the GDPR by virtue of Article 3(2) in respect of that processing.

98 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 micro enterprise 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.

99 Articles 58, 77, 79, 82 and 83 of the GDPR

100 Adopted by the EDPB on 12 November 2019

Example: A US company (being a data controller) has developed a health and lifestyle app, collecting and analysing users' sleep time, weight, blood pressure, heartbeat, etc. to provide health advice. The app is made available to, and is used by, individuals in the EU. For the purpose of data storage, the US company engages a cloud service provider established in the US as a processor.

As the US company is monitoring the behaviour of individuals in the EU in operating the health and lifestyle app, its processing will fall within the scope of Article 3(2) of the GDPR. In carrying out the processing on instructions from, and on behalf of, the US company, the cloud service provider is carrying out a processing activity 'relating to' the targeting of individuals in the EU by its controller. This processing activity by the processor on behalf of its controller falls within the scope of the GDPR under Article 3(2).

(adopted from the *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)*)

Organisations and businesses acting merely as data processors¹⁰¹ in Hong Kong are not directly regulated under the PDPO¹⁰². 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 data¹⁰³. Their principals will be held accountable for the infringing acts or practices performed on their behalf with express or implied authority¹⁰⁴. With regard to data protection on outsourcing activities, the PCPD has published the *Information Leaflet: Outsourcing the Processing of Personal Data to Data Processors* to assist organisations with the recommended contractual and noncontractual measures¹⁰⁵.

101 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).

102 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.

103 Pursuant to DPP2(3) and 4(2) in Schedule 1 to the PDPO

104 Section 65(2) of the PDPO

105 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 and businesses to give individuals a range of prescribed information about the processing of their personal data subject to certain exceptions¹⁰⁶. The prescribed information must be presented in a concise, transparent, intelligible and easily accessible manner. Hence, organisations and 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 includes¹⁰⁷:

<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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 supervisory authority 	<ul style="list-style-type: none"> • whether provision of data is mandatory and consequence of non-provision • information on cross-jurisdiction data transfers • source of data (if not collected from the individual)
--	---	--

¹⁰⁶ 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.

¹⁰⁷ Articles 13 and 14 of the GDPR

In Hong Kong, while organisations and 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 regard¹⁰⁸, the PDPO is less extensive in terms of the items of prescribed information to be notified to the individuals. 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 exceptions¹⁰⁹.

Organisations and 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 likely prejudice the exempted purposes under Part 8 of the PDPO¹¹⁰.

b. Enhanced Right to Erasure ("Right to be Forgotten")

The right to erasure (also known as the "right to be forgotten")¹¹¹ under the GDPR gives an individual a right to require organisations and 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.

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 data¹¹².

108 See DPP1(3) and 5 in Schedule 1 to the PDPO

109 Article 14 of the GDPR

110 Part 8 of the PDPO provides specific exemptions to the application of the DPPs, including collection, use and access.

111 Article 17 of the GDPR

112 Article 17(2) of the GDPR

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 claims¹¹³.

The *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1) - version for public consultation*¹¹⁴ interprets this right to erasure in the particular context of requesting search engine providers to delist links (**delisting request**). The Guidelines explains the grounds upon which a data subject may rely on when making a delisting request and the exceptions where retention of the data is necessary. It highlights that a delisting request, even if based on valid grounds, does not result in the personal data being completely erased from the source websites but only the deletion of the particular information from the list of search results on the subject search engine when the search is made by the data subject's name.

Given the global nature of the internet and search engines, there is a question as to the territorial scope of the right to be forgotten and the extent to which a delisting request may apply. This question was raised in a case before the Court of Justice of the EU in which Google and the French supervisory authority disputed on whether the search engine company was obliged to apply a delisting request to all its search engine's domain name extensions including those for users outside the EU¹¹⁵. The Court of Justice of the EU decided that a search engine operator should be required to carry out a delisting on the versions of its search engine for the EU Member States only. However, the operator should prevent or discourage users in the EU Member States from accessing the delisted links through other domains.

113 Article 17(3) of the GDPR

114 Adopted by the EDPB on 2 December 2019 for public consultation

115 *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)*, Case C-507/17

In Hong Kong, the requirements related to 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). Contravention of the requirement under section 26 is an offence, punishable by a fine of up to HK\$10,000 but there are exceptions to such obligation where the erasure is prohibited by law or it is against the public interest to erase the data.

c. Enhanced Right to Object to Processing

The GDPR provides the right to object at any time to the processing of one's personal data if the processing is based on the following grounds¹¹⁶:-

- (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.

Processing includes profiling. "**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

¹¹⁶ Article 21 of the GDPR; Other bases for data processing (e.g. consent of data subjects, necessary for performance of a contract) are laid down in Article 6 of the GDPR

Upon receipt of objection to processing activities which are based on grounds (a) and (b) above, the data controller must cease the processing of the personal data (including profiling) of the concerned individual 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)¹¹⁷.

In relation to processing personal data for ground (d) above (i.e. scientific or historical research purposes or statistical purposes), an individual may object by relying on his particular situation unless the processing is necessary for the performance of a task carried out in the public interest¹¹⁸. However, no exception shall apply to processing of personal data purely for direct marketing purpose¹¹⁹ (the above ground (c)).

Under the PDPO, an individual in Hong Kong is not generally given the right to request an organisation or business to stop "processing"¹²⁰ 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 by a data controller who may then store the data only for an interim period¹²¹ 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;

117 Article 21(1) and Recital 69 of the GDPR

118 Article 21(6) of the GDPR

119 Article 21(2) of the GDPR

120 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 "Extra-territorial Application of the GDPR".

121 Article 18 of the GDPR

- 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.

In response to a data correction request, an organisation or 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 data¹²².

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 means¹²³.

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*¹²⁴, 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 compatible¹²⁵.

The PDPO in Hong Kong does not provide equivalent right to restrict processing of personal data or right to data portability. Nonetheless, organisations and businesses are required to comply with data access and correction requests from individuals for their personal data¹²⁶.

122 DPP2(1)(b)(i) of the PDPO

123 Article 20 of the GDPR

124 Issued by the EU WP29 in December 2016

125 Recital 68 of the GDPR

126 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

Certification / Seals

The GDPR requires the supervisory authorities, the EDPB and the European Commission to encourage the establishment of data protection certification mechanisms, data protection seals and marks for the purpose of demonstrating compliance with the law by data controllers and data processors¹²⁷. Certification may be particularly useful to organisations and businesses engaging in cloud computing or multilayer 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 met¹²⁸. It can be issued by either private or public accredited certification bodies, subject to the criteria developed by the supervisory authorities or the EDPB, pursuant to the GDPR. Where the criteria are approved by the EDPB, it may result in a common certification, i.e. the European Data Protection Seal¹²⁹.

Certification is on a voluntary basis. The process of certification should be transparent. The information relating to certification mechanism will be maintained in a publicly available register.

A certification does not reduce the responsibility of the data controller or the data processor for compliance with the GDPR and is without prejudice to the tasks and powers of the supervisory authorities.

The *Guidelines on certification and identifying certification criteria* were issued by the EDPB in June 2019¹³⁰. However, as at the end of May 2020, no certification mechanism has been established under the GDPR. In December 2019, the Information Commissioner's Office of the UK announced that it would work with UK Accreditation Service to deliver certification schemes.

127 Article 42(1) of the GDPR

128 Article 42(7) of the GDPR

129 Article 42(5) of the GDPR

130 EDPB, *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation* adopted on 4 June 2019

Codes of Conduct

The GDPR also encourages the drawing up of sector-specific codes of conduct by associations and other bodies to contribute to the proper application of the GDPR, taking into account the features of various processing sectors, and the needs of micro, small and medium-sized enterprises¹³¹. The supervisory authorities of EU Member States shall approve or give comments on whether the code of conduct submitted complies with the GDPR. However, as at the end of May 2020, no code of conduct has been approved under the GDPR.

In Hong Kong, Part 3 of the PDPO also provides for the approval of codes of practice by the PCPD after consultation with the relevant bodies representative of data users and interested parties¹³².

b. Cross-jurisdiction Data Transfer

Transfer of personal data to third countries or international organisations outside the EU continues to be regulated under the GDPR¹³³. Such transfer is permissible if the receiving countries or international organisations have obtained adequacy decisions¹³⁴ from the European Commission¹³⁵ or if the transfer is subject to "appropriate safeguards"¹³⁶. The requirements under the EU Directive are largely preserved in the GDPR in this regard.

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 transferred¹³⁷. The EDPB is required to provide the European Commission with an opinion assessing the adequacy of a country or international organisation's level of protection¹³⁸. As at the end of May 2020, the European Commission has issued adequacy decisions to

131 Article 40 of the GDPR

132 Section 12 of the PDPO

133 Chapter V of the GDPR

134 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)

135 Articles 45 of the GDPR

136 Articles 46 of the GDPR

137 Article 45 of the GDPR

138 Article 45(2) of the GDPR

13 jurisdictions¹³⁹. However, except for Japan, the adequacy decisions of the remaining 12 jurisdictions are based on the EU Directive rather than the GDPR.

In the absence of an adequacy decision made by the European Commission, the mechanisms or safeguards that may be relied on for cross-jurisdictional data transfer include adopting standard contractual clauses and binding corporate rules approved by the EU, as well as approved certification or code of conduct combined with binding and enforceable commitments by the data controllers / data processors in the third country to apply those appropriate safeguards¹⁴⁰.

In Hong Kong, section 33 of the PDPO prohibits transfer of personal data out of Hong Kong unless certain conditions are met, such as when adequate safeguards are in place to protect the transferred data in the destinations. Section 33 has not yet entered into operation. It does not expressly refer to certification or code of conduct as adequate safeguard for cross-jurisdictional data transfer.

¹³⁹ The 13 jurisdictions are Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework). As at the end of May 2020, adequacy talks are ongoing with South Korea.

¹⁴⁰ 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)¹⁴¹ :-

- (a) obtaining parental consent for processing of children's personal data;
- (b) processing personal data anonymously if it is not necessary to identify the data subjects;
- (c) giving data breach notification;
- (d) conducting data protection impact assessment; and
- (e) 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)¹⁴² :-

- (a) complying with the basic principles for processing, such as processing personal data lawfully, fairly and in a transparent manner;
- (b) processing personal data with a lawful basis, such as valid consent;
- (c) 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
- (d) transferring personal data to a recipient in a third country or international organisation pursuant to the lawful mechanisms.

141 See Article 8; Article 11; Article 33; Article 35 and Article 37 of the GDPR

142 See Articles 5-6; Articles 13-22 and Articles 44-49 of the GDPR

Most supervisory authorities in the EU have exercised their power to impose administrative fines in the first two year of implementation of the GDPR. Most of the fines related to violation of the following requirements:

- principles relating to processing of personal data (Article 5);
- lawfulness of processing (Article 6);
- conditions for consent (Article 7);
- processing of sensitive personal data (Article 9);
- transparency and rights of the data subjects (Articles 12 to 22); and
- security of processing and data breaches (Articles 32 to 34)¹⁴³.

Some notable administrative fines include the following:

- €50 million fine was imposed by the supervisory authority of France on an online search engine for lack of transparency and valid consent regarding the use of personal data for advertisement personalisation¹⁴⁴. Information provided by the online search engine on advertisement personalisation was found to be unclear, not comprehensive and not easily accessible by individual users. Moreover, the box indicating users' consent was pre-ticked.
- €27.8 million fine was imposed by the supervisory authority of Italy on a telecommunications company for unlawful processing of personal data for marketing purpose which had affected millions of people. Violations included making marketing calls without valid consent and lack of accountability in managing the relevant personal data¹⁴⁵.
- €14.5 million fine was imposed by the supervisory authority of Berlin, Germany on a real estate company for retaining the unnecessary personal data of its tenants. The company was also unable to demonstrate data protection by design and by default due to its failure to take proper actions to clean up its database after being warned by the supervisory authority¹⁴⁶.

143 EDPB, 'Contribution of the EDPB to the evaluation of the GDPR under Article 97' adopted on 18 February 2020

144 News published by the EDPB on 21 January 2019, available at https://edpb.europa.eu/news/national-news_en

145 News published by the EDPB on 1 February 2020, available at https://edpb.europa.eu/news/national-news_en

146 News published by the EDPB on 5 November 2019, available at https://edpb.europa.eu/news/national-news_en

Other administrative fines in the pipeline include the intention of the Information Commissioner's Office of the UK to fine an airline and a hotel group for data breaches. The intended amounts of fine are £183 million and £99 million respectively¹⁴⁷.

Although Article 83(2) of the GDPR sets out a list of factors for deciding the amount of administrative fine, the levels of fine imposed by different supervisory authorities may vary greatly even for similar violations. EU-wide guidelines on administrative fines may be established by the EDPB. Currently, the supervisory authorities of Germany and the Netherlands have established their own guidelines.

In Hong Kong, if an organisation or business fails to comply with a requirement under the PDPO (including the DPPs in Schedule 1), PCPD 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 offence¹⁴⁸. 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 PCPD does not currently possess the power to impose administrative fines.

¹⁴⁷ In July 2019, the Information Commissioner's Office of the UK announced that it had issued two notices of intention to fine a hotel group of £99 million and an airline of £183 million respectively. The fine of the hotel group related to a cyber incident notified to the Information Commissioner's Office by the group in November 2018, in which approximately 339 million guest records were affected globally. The fine of the airline related to a cyber incident notified to the Information Commissioner's Office by the airline in September 2018, in which personal data of approximately 500,000 customers were compromised. As at the end of May 2020, the two fines were not finalised.

¹⁴⁸ Section 50A of the PDPO





MORE INFORMATION ON THE GDPR





The EDPB is an independent EU body established by the GDPR to promote consistency and cooperation in the enforcement of the law. It also issues guidelines for compliance with the requirements of the GDPR. Members of the EDPB include representatives of the national supervisory authorities of the EU Member States and the European Data Protection Supervisor.

For more information on compliance with the GDPR, organisations and businesses may refer to the websites of the European Commission (http://ec.europa.eu/justice/data-protection/index_en.htm) and the EDPB (https://edpb.europa.eu/edpb_en).





A specific webpage on the GDPR, with major updates, can also be found on PCPD's website (https://www.pcpd.org.hk/english/data_privacy_law/eu/eu.html).

EU GDPR and HK PDPO (Major Differences)

	EU	HK
Application 	Data processors or controllers: <ul style="list-style-type: none"> • with an establishment in the EU, or • established outside the EU, that offer goods or services to, or monitor the behaviour of individuals in the EU. [Art 3] 	Data users (controllers/processors) who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the personal data in or from Hong Kong. [s.2(1)]
Personal Data 	"Personal data" means <ul style="list-style-type: none"> • any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly. • examples of personal data explicitly identified being extended to include location data and online identifier. [Art 4(1)] 	"Personal data" means any data – <ul style="list-style-type: none"> • relating directly or indirectly to a living individual; • from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and • in a form in which access to or processing of the data is practicable. [s.2(1)]
Accountability and Governance 	Risk-based approach; data controllers are required to: <ul style="list-style-type: none"> • implement technical and organisational measures to ensure compliance [Art 24]; • adopt data protection by design and by default [Art 25]; • conduct data protection impact assessment for high-risk processing [Art 35]; and • (for certain types of organisations) designate Data Protection Officers. [Art 37] 	The accountability principle and the related privacy management measures are not explicitly stated. PCPD 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.
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.

	EU	HK
<p>Consent</p> 	<p>Consent must be</p> <ul style="list-style-type: none"> • freely given, specific and informed; • an unambiguous indication of a data subject's wishes, by statement or by clear affirmative action, which signifies agreement [Art 4(1)]; and • given by a child below 16 (or 13) with parental authorisation. 	<p>Consent is not a pre-requisite for the collection of personal data, unless the personal data is used for a new purpose. [DPP1&3] For other purposes, where consent is also required, consent means express and voluntary consent.</p> <p>No requirement for parental consent.</p>
<p>Breach Notification</p> 	<p>Data controllers are required to notify the authority of a data breach without undue delay (exceptions apply).</p> <p>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]</p>	<p>No mandatory requirement, but notification to PCPD (and data subjects, where appropriate) is recommended in the interest of all stakeholders including data users/controllers and subjects.</p>
<p>Data Processors</p> 	<p>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]</p>	<p>Data processors are not directly regulated. [s.2(12)]</p> <p>Data users are required to adopt contractual or other means to ensure data processors' compliance. [DPP2(3) & DPP4(2)]</p>
<p>New or Enhanced Rights for Data Subjects</p> 	<ul style="list-style-type: none"> • Right to notice on data processing [Art 13-14] • Right to erasure of personal data ("right to be forgotten") [Art 17] 	<ul style="list-style-type: none"> • Less extensive notice requirements for data users/controllers (processors) • No right to erasure, but data shall not be retained longer than necessary [s.26 & DPP 2(2)]

EU GDPR and HK PDPO (Major Differences)

	EU	HK
<p>New or Enhanced Rights for Data Subjects (Cont'd)</p> 	<ul style="list-style-type: none"> • Right to restriction of processing and data portability [Art 18, 20] • Right to object to processing (including profiling) [Art 21] 	<ul style="list-style-type: none"> • 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]
<p>Certification, Seals, and approved Codes of Conduct</p> 	<p>Mechanisms are explicitly recognised and established for demonstrating compliance by data controllers and processors. [Art 42]</p>	<p>No formal recognition of certification or privacy seals mechanisms for demonstrating compliance. PCPD may approve and issue code of practice after consultation. [s.12]</p>
<p>Cross-jurisdiction Data Transfer</p> 	<p>Certification and adherence to approved codes of conduct are explicitly made one of the legal bases for transfer. [Art 46]</p>	<p>Certification and adherence to an approved code of practice are not explicitly made a legal basis.</p>
<p>Sanctions</p> 	<p>Supervisory authorities are empowered to impose administrative fines on data controllers and processors. [Art 58]</p> <p>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]</p>	<p>PCPD is not empowered to impose administrative fines or penalties.</p> <p>PCPD may serve Enforcement Notices on data users, failure to comply with which may attract penalties after judicial process. [s.50]</p>




香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong



私隱公署網頁
PCPD website
pcpd.org.hk



下載本刊物
Download
this publication

查詢熱線 Enquiry Hotline : (852) 2827 2827
 傳真 Fax : (852) 2877 7026
 地址 Address : 香港灣仔皇后大道東248號陽光中心13樓1303室
 Room 1303, 13/F, Sunlight Tower,
 248 Queen's Road East, Wanchai, Hong Kong
 電郵 Email : enquiry@pcpd.org.hk



本刊物使用署名4.0國際(CC BY 4.0)的授權條款，只要你註明原創者為香港個人資料私隱專員，便可自由分享或修改本刊物。詳情請瀏覽creativecommons.org/licenses/by/4.0/deed.zh。

This publication is licensed under Attribution 4.0 International (CC By 4.0) licence. In essence, you are free to share and adapt this publication, as long as you attribute the work to the Privacy Commissioner for Personal Data, Hong Kong. For details, please visit creativecommons.org/licenses/by/4.0.

免責聲明 Disclaimer

本刊物所載的資訊和建議只作一般參考用途，並非為法例的應用提供詳盡指引，亦不構成法律或其他專業意見。私隱專員並沒有就本刊物內所載的資訊和建議的準確性或個別目的或使用的適用性作出明示或隱含保證。相關資訊和建議不會影響私隱專員在《個人資料(私隱)條例》下獲賦予的職能及權力。

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 and do not constitute legal or other professional advice. 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.

二零一八年三月初版 First published in March 2018
 二零二零年五月(第一修訂版) May 2020 (First Revision)

