■ 資料來源：香港個人資料私隱專員公署

歐洲聯盟《通用數據保障條例》2016（於2018年5月25日生效）

歐洲聯盟《通用數據保障條例》於2016年被採納，並於2018年5月25日生效。此條例會取代現時歐洲議會及理事會第95/46/EC號指令（歐盟指令）訂明的資料保障規例，而且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。

香港個人資料私隱專員黃繼兒早前發出歐洲聯盟《通用數據保障條例》2016小冊子，以提高香港機構／企業對歐盟新制定的資料保障監管框架的認識，並了解其可能帶來的影響，同時就當中部分主要的規定與香港法例第486章《個人資料（私隱）條例》（《私隱條例》）作出比較。

歐盟是香港第二大的貿易夥伴，而《通用數據保障條例》下的域外應用則規定只要香港機構／企業涉及收集和處理歐盟人士的個人資料，便須為遵從此條例的規定作好準備。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，包括協調及簡化現時的單一數碼市場框架；讓個人掌握他們的資料；及制定現代化的保障資料管治規範。

為何《通用數據保障條例》與香港的機構／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年的私隱指引及歐盟指令。故此，《私隱條例》與《通用數據保障條例》有很多共通點。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／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。

《通用數據保障條例》的域外應用

《通用數據保障條例》與現時的規定有明顯分別，香港的機構／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；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。

若一家機構／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。

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

《通用數據保障條例》亦適用於在**歐盟以外的法域區**（包括香港）設立的機構／企業所進行涉及處理個人資料的活動。

香港個人資料私隱專員黃繼兒表示，歐盟是香港第二大的貿易夥伴，不少香港企業的業務或交易模式已走向全球化及多元化，相信此小冊子能夠讓企業了解其業務會否抵觸新條例的規定。

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**的角色處理個人資料的機構／企業，不論有關個人資料是否真正在歐盟境內處理。

《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**。

即使香港的機構／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／企業也可能會受《通用數據保障條例》影響。

若要確定機構／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)

《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」。

> 《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)。

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。

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／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。

在展示循規方面，機構／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；
- 進行**資料保障影響評估**，以識別及管理資料保障風險；
- 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；
- 為資料處理活動保存**記錄**；及
- 制定資料處理**政策或措施**，以展示循規及問責。

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／措施作紀錄、進行資料保障影響評估)。歐盟的《保障資料主任指引》就委任保障資料主任、所需的專長及技能提供指引。

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：

- 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)；
- 其核心活動包含處理運作時需要對資料當事人作大規模的定期及系統性監察；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。

保障資料主任至少須執行下述工作：

- 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。

UPM Finesse Classic Matt, 90 gsm

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／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。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。

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，惟香港個人資料私隱專員公署鼓勵機構／企業採納私隱管理系統以落實問責原則。機構／企業可採用私隱管理系統作為策略性框架，輔以恒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／企業遵從《私隱條例》的規定。私隱管理系統亦有助機構／企業推行公開和具透明度的資訊政策和措施，以示機構／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。

B. 資料保障影響評估

資料保障影響評估協助資料控制者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。尤其是在下述的情況，必須進行資料保障影響評估：

- 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。

私隱專員已出版《私隱影響評估》資料單張，旨在指導香港的機構／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。

C. 貫徹私隱的設計及預設

機構／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。

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。

D. 資料配對

機構／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。

僱用少於 250 人的機構／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。

機構／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／企業評估接著應如何達致資料保障的管治。

機構／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／企業須令其私隱政策及措施具透明度。

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，較現行的歐盟指令施加較嚴格的規定。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；或 (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。

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／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。

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：

- 資料當事人同意就個別或多個特定目的作處理；或
- 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。（間線標示強調）

當機構／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。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。
- ✘ 綑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。

- ✔ 瀏覽網站的條款及細則時加上剔號。
- ✔ 在智能電話安裝應用程式選擇技術設定。

UPM Finesse Classic Matt, 90 gsm

B. 兒童以電子形式表示同意

機構／企業就處理兒童的個人資料以提供「資訊社會服務」(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。

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／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／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況，與提供服務無關的其他條款或細則綑綁在一起。

至於任何一名處於弱勢的資料當事人並屬於(i)未成年人，(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》並沒有述明可以電子形式給予同意，但容許藉由「有關人士」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的情況下，代他給予訂明同意。

資料外洩事故強制通報

《通用數據保障條例》強制規定機構／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。作為資料處理者的機構／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：

- 事故的性質及可能的後果；
- 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／企業的保障資料主任或其他聯絡人的聯絡資料。

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》，闡述作出通報的步驟。私隱專員建議機構／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，讓他們可立即採取步驟以減低任何可能的傷害。

資料處理者的責任

擔當資料處理者的香港機構／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。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：

- 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。

《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）：

- 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。

就保存紀錄的規定而言，《通用數據保障條例》對僱用少於 250 人的機構／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的特點。

根據《通用數據保障條例》，資料處理者是直接受資料保障機構所規管，違反責任（例如沒有通報資料外洩事故）可被判罰。

在香港，只作為資料處理者的機構／企業，並不直接受《私隱條例》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。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。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方面，為機構／企業提供建議。

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，《通用數據保障條例》規定機構／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／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：

• 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	• 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 • 向相關資料保障機構投訴的權利	• 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）

UPM Finesse Classic Matt, 90 gsm

在香港，雖然機構／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，惟《私隱條例》就處理個人資料方面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。

私隱專員鼓勵香港的機構／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》第八部所載的目的，《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。

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」）讓個人在指定情況下有權要求機構／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。

《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。

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。《私隱條例》第26條為這項責任提供例外情況，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，個人有權隨時根據下述理由反對處理其個人資料，包括個人概況彙編：

(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。

《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。

資料控制者在收到反對根據上述 (a) 及 (b) 理由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合法理據，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）。

有關根據上述 (d) 理由（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。不過，純粹為直接促銷目的而處理個人資料，則沒有例外情況可適用。

根據《私隱條例》，一名個人在香港一般無權要求機構／企業停止「處理」其個人資料，但機構／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／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／企業若曾在過往的12個月內向第三方提供有關不準確的資料，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。

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。

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》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。

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／企業須依從個人所提出有關查閱及改正其個人資料的要求。

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

《通用數據保障條例》明確確認以私隱印章或標誌以證明其符合法規要求。作為規管機構的歐洲資料保障委員會（取代第29條資料保障工作小組）及歐盟委員會將鼓勵建立資料保障認證機制，讓資料控制者及資料處理者顯示其循規守法。認證制度可能適用於從事雲端運算或多層資料處理的機構／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。認證可由私營或公營認證機構按資料保障機構所制訂的準則而發出，或由歐洲資料保障委員會依據《通用數據保障條例》發出。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。

認證屬自願性質。有關認證的資訊須具透明度，而認證標記亦會備存於公共登記冊內。

UPM Finesse Classic Matt, 90 gsm

另一方面，《通用數據保障條例》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，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。在這方面，《私隱條例》第三部亦訂明，香港的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。

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。個人資料或會轉移至歐盟以外能提供足夠資料保障的國家或國際機構。歐盟指令在這方面的原有規定，大部分獲得保留。

此外，採納認證機制或經核准的行為守則內的個人資料保障措施，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，便可構成把個人資料轉移至歐盟以外的司法管轄區的其中一個基礎。

《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。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。

在歐盟委員會尚未作出資料保障足夠度的評估決定時，國際轉移資料可援引的機制或安全措施（除了認證機制）還包括採用歐盟核准的標準合約條款及企業約束規則。然而，《私隱條例》沒有明確提及認證機制或私隱印章／標誌。

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1,000萬歐元，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）：

(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2,000萬歐元，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）：

(a) 遵從資料處理的基本原則，例如合法及公平地處理或以同意作為基礎而進行處理；
(b) 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
(c) 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。

在香港，如機構／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／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。《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，私隱專員無權施加行政罰款。

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： • 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： • 任何有關一名已被識別或可被識別的自然人的資訊；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： • 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： • 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。
同意	同意必須是 • 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。	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。 沒有規定需要家長同意。
通報資料外洩事故	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）。 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]	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）。

	歐盟	香港
資料處理者	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]	資料處理者不是直接受規管。[第2(12)條] 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]
資料當事人新增及提升的權利	• 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]	• 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《條例》中亦有條文規管資料核對程序。[第30-31條]
認證、印章及行為守則	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]	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]
司法管轄區之間的資料轉移	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]	認證制度及依從實務守則未有明確定為法律基礎。
懲罰	資料保障機構獲授權可判處資料控制者及處理者行政罰款。[第58條] 視乎違規的性質，罰款可達2,000萬歐元或全球年度總營業額的4%。[第83條]	私隱專員沒有獲賦權施加行政罰款或刑罰。 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]

機構／企業可參考歐盟委員會的保障個人資料網站〈ec.europa.eu/info/law/law-topic/data-protection_en〉，或香港個人資料私隱專員公署的網頁〈www.pcpd.org.hk/tc_chi/data_privacy_law/eu/eu.html〉，了解更多詳情及相關的指引資料。如有查詢，請參閱以下聯絡資料：

香港個人資料私隱專員公署

熱線：+852 2827 2827
傳真：+852 2877 7026
電郵：enquiry@pcpd.org.hk
地址：香港灣仔皇后大道東248號陽光中心12樓