歐洲聯盟《通用數據保障條例》

簡介

什麼是《通用數據保障條例》？

《通用數據保障條例》由歐洲聯盟（歐盟）制定，並於2018年5月25日生效，目的是保障歐盟公民的個人資料和提升相關權利。

條例會對誰及如何帶來影響？

香港機構即使在歐盟沒有設立機關，如在下列情況下處理歐盟人士的個人資料，也可能需遵從《通用數據保障條例》的規定：

1) 向歐盟人士提供（收費或免費）貨品或服務；或
2) 監察歐盟人士在歐盟內的行為。

違規會帶來什麼懲罰？

最高行政罰款可達2,000萬歐元或全球年度總營業額的4%，以較高者為準。

重點

域外應用：《通用數據保障條例》適用於在歐盟以外的司法管轄區（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。

「個人資料」的定義：「個人資料」的定義擴大至包括任何有關一名已被識別或可被識別的自然人的資料，例如姓名、地址、身份識別號碼、位置資料、網上識別代號，如小型文字檔案(cookies)及互聯網規約(IP)地址、聲音和錄像記錄、靜止圖像等。

特別類別的個人資料：「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，以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。

透明度及同意：《通用數據保障條例》規定資料控制者以清晰簡單的語言向資料當事人提供有關處理其個人資料的詳盡資訊，並須向他們提供真正及分項的選擇，讓他們以不含糊的通知或清晰肯定的行動就不同的資料處理活動個別地給予同意。

提升的個人權利：《通用數據保障條例》提升個人各方面的權利。資料當事人有在資料處理方面獲通知的權利；個人資料查閱、修改或刪除的權利、限制或反對處理的權利、資料可攜權，以及不接受以基於自動化處理（包括個人概況彙編）所作決定的權利。

資料外泄及應變：《通用數據保障條例》規定資料控制者向歐盟成員國的監管機構通報資料外泄事故，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）。如有關事故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，不可延誤。

貫徹私隱的設計及預設設定：《通用數據保障條例》規定資料控制者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。

作好準備

機構／企業須 (i) 展示其遵從處理個人資料的原則[1]；(ii) 實施適當的技術性及機構性措施以確保循規[2]；以及 (iii) 在處理的過程中納入對資料的保障[3]。具體而言，應在資料保障過程中實施或納入以下措施：

- 委任保障資料主任[4]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；以及
- 制定資料處理政策或措施，以展示循規及問責。

*註1, 2, 3：分別根據《通用數據保障條例》第5(2)條、第24條以及第25條。
註4：如處理個人資料不是業務的核心部分和有關活動沒有對個人構成風險，若干在《通用數據保障條例》下的責任並不適用，例如委任保障資料主任。

例子

《通用數據保障條例》適用情況

你的機構是一間在歐盟以外成立並於網上營運的小規模高等教育機構，主要以歐盟以內的西班牙語和葡萄牙語大學為對象，並就一些大學課程提供免費意見。學生需要用戶名稱及密碼以取得你的機構的網上材料。學生填妥報名表後，你的機構會提供所需的用戶名稱及密碼。在此情況下，《通用數據保障條例》便會適用。

《通用數據保障條例》不適用情況

你的機構是一個設於歐盟以外的服務提供者，為歐盟以外的客戶提供服務。當你的客戶到其他國家（包括歐盟國家）旅遊時可使用你的服務。假使你的機構沒有特別以歐盟人士為服務對象，《通用數據保障條例》便不適用。

延伸閱讀

EU GDPR	*https://ec.europa.eu/info/law/law-topic/data-protection_en*
UK ICO	*https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/*
HK PCPD	*https://www.pcpd.org.hk/tc_chi/data_privacy_law/eu/eu.html*