為《通用資料保障條例》做好安排

資料來源: 工商月刊 (2018 年 7 月號)
翰宇國際律師事務所合夥人陳曉峰

擁有歐洲客戶的香港公司不可忽視歐盟的最新條例

「我們近日已按《通用資料保障條例》更新私隱政策。請按此確認您接受我們最新的私隱政策。」 你的收件箱最近有否被類似的電郵淹沒？當你流覽 網頁時，有否留意到視窗彈出了大量有關隱私的通知？

在香港，許多人大可不必深究背後原因，直接按下「接受」。然而，這些視窗不斷湧現乃因《通用資料保障條例》（GDPR） 這一冗長的新條例近日正式生效，港企絕對不容忽視。

違反 GDPR 最高可被罰款 2,000 萬歐元（港幣 1.8 億元），或 公司全球年營業額的 4%（以金額較高者為准）。

GDPR 為歐盟法律下有關資料保障和隱私的條例，於 5 月 25 日生效。

很多港企或會有以下想法：

- 我們的公司不在歐盟，因此 GDPR 與我們無關。
- 不用擔心，讓歐盟的分公司處理 GDPR 便可。
- 我們的合約不受歐盟成員國的法律約束，因此 GDPR 不適用 於我們。

他們有這些想法亦可以理解，但事實是 GDPR 仍適用於在香 港境外經營的港企。

GDPR 的全球影響

GDPR 有別於其他法例和條例，具有域外效力，其影響遍及全球。

例如，處理有關提供貨物及服務或監察自然人行為的資料時，GDPR 適用於處理身在歐盟的自然人之個人資料，即使處理該等資料的人士或公司並不位於歐盟。

例子舉隅

在網上銷售貨品的香港公司：倘在歐盟境外成立的公司透過其官方網站向身在德國的德國公民銷售貨品，或該網站監察該 德國公民的行為，則該公司須遵守 GDPR。

經營雲端服務儲存系統的香港公司：例如，客戶（部分來自 歐盟）的個人資料提供予香港公司經營的雲端服務儲存系統。 由於歐盟境內可進入該雲端系統，加上該等身在歐盟的人士之個人資料將轉移到香港作備存，然後再轉移至協力廠商作進一步處理，因此香港公司處理該等些歐盟人士的個人資料，以及與 該等客戶和任何協力廠商處理者所簽訂的合約之有關條款，必須符合 GDPR。

誰人受到該條例保障？

港企必須考慮的另一問題為：GDPR 是否適用於所有身處歐盟的人士？

到底 GDPR 只適用于歐盟公民，抑或適用於所有在個人資料被收集時身處歐盟的人士，是備受爭議的問題。GDPR 內文列明，條例不僅適用於處理個人資料的歐盟公司，還適用于歐盟境外的公司。看來該條例並不把資料當事人局限于歐盟公民或居民。

就此，各方有不同詮釋。為審慎起見，我們建議企業應保持謹慎，假定條例適用於所有在個人資料被收集時身處歐盟的人士，尤其是當公司在全球各地均有業務，並與不同集團公司互 相轉移資料。

部分企業或表示並無打算向身在歐盟的人士提供任何服務。就此，條例的適用性將按每宗個案的情況而定，當中的考慮因素包括所涉及的語言（如網上商店有否提供任何歐盟語言）、貨幣（如價錢是否以歐元標示），以及有否提及任何身處歐盟的顧客。

資料當事人的額外保障

GDPR 賦予資料當事人多項額外權利，包括但不限於反對權、敏感性資料的特殊權利、被遺忘權、資料外泄通知，以及詳細列明所收集和處理的個人資料類別之需要。此等權利本身極其複雜，本文不在此贅。

GDPR 的實施

GDPR 生效當天，WhatsApp、Facebook、Google 和 Instagram 都捲入因新法例而起的訴訟。Facebook 就被要求罰 款 430 億美元。蘋果、亞馬遜和 LinkedIn 等企業亦被起訴，預期更多申訴將陸續有來。

鑒於觸犯 GDPR 的潛在風險甚高，我們察覺到部分歐盟境外的企業如《洛杉磯時報》和《今日美國》，已決定封鎖歐盟訪客。

其他已採取的措施包括要求客戶聲明自己並非身處歐盟，以及提供不含 cookies 的純文字版網站，以防在不經意的情況下收集了個人資料。

然而，此舉卻有如「斬腳趾避沙蟲」。事實上，封鎖所有歐 盟 IP 能否徹底避免 GDPR 的法律責任仍然成疑。對歐盟這個全球 最大經濟體之一避而遠之，在商業上也不大合理。

港企的對策？

港企可採取甚麼措施，確保遵守 GDPR？

這並不是在資料政策中附加 GDPR 參考資料便可簡單了事。（即使沒有 GDPR，我們也強烈建議企業根據香港《個人資料(私隱)條例》制訂資料私隱政策。）

倘企業與歐盟人士進行任何商業活動或交易，則應就其活動作出評估，以確認是否受到 GDPR 約束。若企業須遵守條例，則應採取一切必要措施，確保該等活動符合 GDPR。

港企可採取的措施包括：

1. 更新資料私隱政策；
2. 確保與附屬公司訂立適當的合約條款（如把歐盟附屬公司持有的雇員資料轉移至香港總部，或服務供應商處理歐盟資料 當事人的個人資料）；
3. 修改現有協議，加入 GDPR 所規定的新合約條文，如審計權、委任次級處理者、保安措施等；
4. 就處理者的保安措施及有否遵循 GDPR 展開盡職調查；及
5. 把網站升級至符合 GDPR 標準。在起草設計時，企業應特別 留意相同的通知應否適用于歐盟境外的客戶。倘企業能偵測歐盟訪客並獨立處理他們的資料，則可另外使用歐盟告示。

鑒於 GDPR 已生效，因此如閣下的業務仍未就 GDPR 進行 任何風險評估，則應立即行動，並進行適當的私隱影響評估。