



【國際】歐盟實施新數據保障條例 港商勢受影響

2018年6月1日

資料來源：節錄自HKTDC

今年5月25日，新的《通用數據保障條例》(General Data Protection Regulation)在歐盟各國直接實施。新法例為保障個人數據建立整套協調一致的規則，取代原有關於數據保障的第95/46/EC號指令及各成員國的實施法例。

如果公司在歐盟提供商品或服務，或者監控數據當事人在歐盟內的行為，即使在歐盟沒有實體存在，也須遵守該條例。監控行為包括使用Cookie來監控網上活動，並建立用戶檔案(即使不知道用戶姓名)。

《通用數據保障條例》建基於現有理念之上，加強對收集和使用個人數據的要求。此外，條例還引入一些重大變化，特別是：

- 管控人有義務記錄為遵守《通用數據保障條例》所採取的措施和決定，以證明合規(即問責原則)。認證和行為守則可以幫助企業證明其遵守條例。
- 許多公司應就處理個人數據的所有活動保存內部登記冊。另一方面，歐盟多個成員國現行的數據處理活動強制登記或通報規定則予取消。
- 關於取得個人「同意」的要求進一步收緊。因此，公司或要對取得同意的機制作出檢討和調整。
- 《通用數據保障條例》更詳細地說明須向當事人提供的資料，以及提供資料的方式。因此，香港企業應更新其向歐洲數據當事人發出的通告，包括網站政策、用戶條款和細則，及/或員工通知。
- 數據當事人的權利得到加強，並獲授予新的權利。其中包括數據當事人有權將數據轉移予另一處理人(即資料可攜性)，以及有權要求數據管控人在某些情況下(如撤回同意或沒有其他處理其數據的法律依據時)刪除其個人數據，不得無故拖延。香港企業須建立程序和流程來處理這些要求。
- 公司必須就數據洩露(如個人數據意外或非法遺失、遭竊取、查閱或披露)發出通報。即是說，個人數據洩露情況須在72小時報告主管當局，特定情況下應通知有關個人。
- 此外，數據處理人(即代表其他公司處理個人數據的公司)應就遵守《通用數據保障條例》下的各項義務直接負責，並承擔責任，包括確保個人數據在技術及組織上得到保障。管控人也須更新與處理人之間的合同。
- 對香港公司而言，重要的是《通用數據保障條例》規定在歐盟以外成立的公司須在歐盟成員國委任代表。

違規後果：《通用數據保障條例》屬強制性，公司必須遵守，而且對其聲譽至關重要。公司若未能履行該條例下的法律義務，可被處罰，包括罰款高達2,000萬歐元，或其全球營業額的4%(以較高者為準)。數據保障主管當局也有權命令公司放棄或修改其違規的數據處理操作，此舉可能導致公司的業務中斷，損失不菲。

此外，任何數據當事人若因公司違規而受損，可通過集體訴訟等方式向該公司索償。再者，世界各地日益認識到保障個人數據的重要性，因此，如果公司未能充分保障這些數據，不可避免會損害其聲譽和業務。