


# 雲端的法規，教育與未來展望

## 第三組

# 雲端的法規：

根據香港個人資料私隱專員公署的法規：



資料使用者須依從條例的規定，包括附表1的保障資料原則。在聘用雲端服務供應商時，保障資料**第2(3)、3、4原則**及條例**第65(2)條**尤其相關。

**保障資料第2(3)原則**規定，如資料使用者聘用（不論在香港或香港以外聘用）資料處理者，以代該資料使用者處理個人資料，該資料使用者須採取合約規範方法或其他方法，以防止轉移予該資料處理者的個人資料的保存時間超過處理該資料所需的時間<sup>1</sup>。

**保障資料第3原則**規定，個人資料不應用於新目的，除非已取得資料當事人或其「有關人士」（如條例下的定義）的訂明同意（即明確及自願的同意）。

**保障資料第4(1)原則**規定，資料使用者須採取所有合理地切實可行的步驟，以確保由其持有的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響，尤其須考慮：

- (a) 該資料的種類及如該等事情發生便能造成的損害；
- (b) 儲存該資料的地點；
- (c) 儲存該資料的設備所包含（不論是藉自動化方法或其他方法）的保安措施；
- (d) 為確保能查閱該資料的人的良好操守、審慎態度及辦事能力而採取的措施；及
- (e) 為確保在保安良好的情況下傳送該資料而採取的措施。

**保障資料第4(2)原則**規定，如資料使用者聘用（不論在香港或香港以外聘用）資料處理者，以代該資料使用者處理個人資料，該資料使用者須採取合約規範方法或其他方法，以防止轉移予該資料處理者作處理的個人資料未獲准許或意外地被查閱、處理、刪除、喪失或使用<sup>2</sup>。

**條例第65(2)條**規定，資料使用者的承辦商（例如雲端服務供應商）所作出的資料外洩或濫用的行為，會被視為亦是由該資料使用者及其承辦商作出的。換言之，資料使用者須對其承辦商的作為負上責任。

根據保障資料第2(3)、3、4原則及條例第65(2)條，資料使用者須保護資料當事人交託予他們的個人資料，防止資料被濫用，不論有關個人資料是否儲存於資料使用者的處所，抑或外判予承辦商或雲端服務供應商。

# 如何加強對雲端服務的安全教育：

雲端工作人員應該要避免這些錯誤行為：

- 避免資料暴露或洩露
- 不要來自組織外部的未經授權使用者擁有了對內部資料的存取權限
- 加強打擊雲端的漏洞，才能削弱或損毀了雲端基礎結構和惡意攻擊（例如 DDoS 攻擊或惡意軟體感染）
- 不要過多內部授權使用者對內部資料的存取權限

# 雲端服務的教育或培訓措施可以實施：

- 個性化學習

雲端技術可以幫助收集和分析學生/學員的學習數據,從而提供個性化的學習建議和輔導。教師可以根據學習者的進度、興趣等因素,為他們設計更加貼合需求的教學方案。

- 智能評估和反饋

雲端系統可以自動評估學習者的表現,給予及時的反饋,幫助他們及時發現和改正問題。同時也可以提供數據分析,供教師優化教學方法。

虛擬實驗室和模擬環境

## 雲端的不同教育措施的效果和覆蓋範：

- 個性化學習

效果:根據學習者的個人需求和特點,提供更有針對性的教學方案,顯著提高了學習效果。

覆蓋範圍:主要集中在K-12教育和職業培訓領域,部分高等教育機構也開始採用。

- 智能評估和反饋

效果:大幅提高了評估的效率和客觀性,並能及時發現問題,為教學改進提供依據。

覆蓋範圍:適用於各類教育機構,目前應用最普遍的是K-12學校和職業培訓機構。

# 雲端的未來展望：

## 雲端針對該新興技術，未來可能面臨的網絡安全挑戰有哪些？

### 1.數據安全和隱私保護：

挑戰:大量敏感的個人和教育數據存儲在雲端，面臨遭到非法存取、泄露或遺失的風險。

防禦策略:採用加密、身份驗證、權限管控等措施，並制定詳細的數據備份和災難恢復計劃。

### 2.系統漏洞和網絡攻擊：

挑戰:雲端系統可能存在安全漏洞，容易遭受黑客入侵、病毒感染、DDoS攻擊等。

防禦策略:定期更新修補系統漏洞，部署防火牆和入侵檢測系統，提高網絡安全意識。

### 3.供應鏈安全：

挑戰:雲服務供應商、教學內容提供商等各環節存在潛在安全風險。

防禦策略:嚴格審核供應商資質和安全措施，建立多層級安全防護體系。

Q&A