

切勿輕視個人資料保安 Personal data security must be taken seriously

旅遊業界必須做好客戶個人資料的保安工作，藉以彰顯良好的企業管治，建立優良商譽，贏取客戶信任。

The travel industry must safeguard customers' personal data to demonstrate good corporate governance, thereby building up a credible reputation and earning trust from customers.

個人資料私隱專員公署 *The office of the Privacy Commissioner for Personal Data (PCPD)*

旅行社在日常營運中收集和保存客戶大量的個人資料，因此必須致力預防資料外洩，而萬一資料外洩，必須致力減輕影響，以免商譽受損，客戶流失。

個人資料的保安

機構身為資料使用者，必須採取所有切實可行的步驟，以保障客戶的個人資料不會在未經授權或意外情況下被查閱、處理、刪除、喪失或使用，否則便有可能違反《個人資料(私隱)條例》下的「資料保安原則」(六項「保障資料原則」之一)。

此外，若機構聘用身處香港或在香港以外地方的資料處理者處理個人資料，必須採取合約規範方式或其他方法，以防止轉移予該資料處理者作處理的個人資料在未經授權或意外的情況下被查閱、處理、刪除、喪失或使用。

「資料保安原則」的重點，是機構是否已採取「所有切實可行的步驟」以確保所持有個人資料的安全。因此，即使有個人資料外洩，亦不一定等於資料使用者已違反了這項「保障資料原則」。私隱專員公署會從多方面去檢視機構是否已採取所有切實可行的步驟，包括：

With a vast amount of customers' personal data collected and retained in their daily operation, travel agents must strive to prevent data breaches or, should there be such breaches, minimise the impact in order to avoid damage to reputation and customer defection.

Security of personal data

Organisations as data users should take all practicable steps to ensure that customers' personal data is protected against unauthorised or accidental access, processing, erasure, loss or use, or they may contravene the Data Security Principle (one of the six Data Protection Principles) under the Personal Data (Privacy) Ordinance.

In addition, if organisations engage data processors, whether within or outside Hong Kong, to process personal data on their behalf, the organisations must adopt contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processors for processing.

The essence of the Data Security Principle is whether an organisation has taken "all practicable steps" to ensure the security of personal data. Therefore, a data breach incident does not necessarily equate to this Data Protection Principle having been contravened by the data user. The PCPD will evaluate from various aspects to consider whether an organisation has taken all practicable steps, including:

- **Organisational preventive measures**, such as consistency of application of personal data privacy protection in corporate governance


- **組織層面上的預防措施**，如在企業管治方面貫徹執行個人資料私隱保障(涵蓋業務常規、操作程序、政策、培訓等)，有整全的檢討及監察程序，以及有公開和具透明度的資訊政策和常規等。
- **技術層面上的保安措施**，如實行資訊系統、網絡基礎設施等的保安工作；定期對保安系統的政策和程序，以及有關進入系統、傳送和保存資料的保安措施和步驟加以審視；以及採用國際上接受的準則和技術等。
- **資料外洩事故發生後的處理步驟**，即如何處理善後工作，包括補救措施，如何通知受影響的資料當事人，以及如何防止事故再次發生等。

資料外洩的處理及通報

機構若發現資料外洩，私隱專員公署鼓勵有關機構儘早作出資料外洩事故通報。通報資料外洩事故有利於公署與相關機構合力減低因事件而構成的潛在損害，並尋求改善方案以免事件再次發生。公署刊發的《資料外洩事故的處理及通報指引》，建議發生資料外洩事故時，機構可依從以下四個步驟處理：

- **立即收集資料**：如事故於何時何地發生、事故肇因、所涉及個人資料的種類及範圍、受影響人數等。
- **聯絡相關人士及採取遏止措施**：相關人士可包括執法部門、相關規管機構(如私隱專員)、互聯網公司及資訊科技專家；遏止措施可包括停止有關系統的操作、更改用戶密碼及系統配置、修補系統的漏洞、保留資料外洩的證據以協助調查等。
- **評估可能造成的損害**：如人身安全、身份盜竊、財務損失等。
- **考慮作出資料外洩事故通報**：包括通知資料當事人及相關人士。

業界機構應建立自己的私隱管理系統，把個人資料私隱保障納入企業管治責任，並由上而下加以推行，從「合規」擢升為「問責」，藉以贏取僱員和客戶的信任和稱許。

如需更多詳細資料，可瀏覽私隱專員公署網站(www.PCPD.org.hk)。為協助中小企業加強保障個人資料，公署設立了諮詢熱線(2110-1155)和電郵信箱(sme@pccpd.org.hk)，歡迎業界中小企業向公署查詢。 

(covering business practices, operational procedures, policies, training, etc), comprehensive review and monitoring procedures, as well as open and transparent data policies and practices, etc.

- **Technical security measures**, such as implementation of security measures on information systems and network infrastructure facilities; regular review of policies and procedures of security systems, and security measures and procedures on system access, data transfer and storage; as well as implementation of widely accepted international standards and technology, etc.
- **Mitigating steps after data breaches**, i.e. how to respond to the data breach incidents, including remedial measures, ways to notify data subjects affected and preventive measures, etc.

Data breach handling and notifications

In the event of a data breach, the organisation is strongly advised to give data breach notifications (DBNs) as early as possible, so that the PCPD can join hands with the organisation to minimise potential adverse impact caused by the incident, and to look for improvements to prevent further breaches. The PCPD has issued the "Guidance on Data Breach Handling and the Giving of Breach Notification", which recommends the following four-step action plan for handling data breaches:

- **Collecting information immediately**: e.g. when and where did the breach take place? What was the cause? What kind and extent of personal data was involved? How many data subjects were affected?
- **Contacting the interested parties and adopting containment measures**: interested parties may include law enforcement agencies, relevant regulators (e.g. the Privacy Commissioner), Internet companies and IT experts; and containment measures may include stopping the relevant system, changing users' passwords and system configurations, remedying the system loopholes, keeping evidence of the data breach to facilitate investigation, etc.
- **Assessing the harm**: e.g. threat to personal safety, identity theft, financial loss, etc.
- **Considering giving notification**: notifying the affected data subjects and the relevant parties.

Organisations of the trade are encouraged to adopt their own privacy management programme to embrace personal data privacy protection as part of their corporate governance responsibilities, and implement it by a top-down approach, marking a shift from compliance to accountability, in order to win the trust and recognition from their employees and customers.

For more information, please visit the PCPD website (www.PCPD.org.hk). To assist the small- and medium-sized enterprises (SMEs) in enhancing personal data protection, the PCPD has launched a dedicated hotline (2110-1155) and email (sme@pccpd.org.hk) service providing convenient and effective channels for SMEs to raise enquiries. 