



# Embracing Privacy and Data Protection as a Part of Corporate Governance in the Boardroom

## 企業管治必須重視

## 私隱與個人資料保障

The Personal Data (Privacy) Ordinance (the Ordinance) came into force in 1996. However, for many years thereafter, privacy and data protection had remained a subject that was not given the attention it deserves.

In the day-to-day management of an organisation, it goes without saying that we need to take care of spending budgets, looking after customer service and public relations, management of staff, and so on. More sophisticated organisations would assume their corporate social responsibilities and assess the environmental impact of their operations. By contrast, privacy and data protection was traditionally accorded a low priority in an organisation's business agenda. This is no longer a viable strategy in an age of "Big Data" and high customer expectations for their privacy rights.

### Growing Importance of Privacy and Data Protection

Hong Kong was the first jurisdiction in Asia to have a dedicated piece of legislation on personal data privacy. As at today, 10 other jurisdictions in the region have similar legislations in force or about to be in force. These include South Korea, Macao, Vietnam, Malaysia, Japan, Taiwan, Thailand, the Philippines, India and Singapore. Globally, at least 102 jurisdictions have comprehensive data protection laws in force or awaiting implementation.

This trend reflects the growing recognition by governments of privacy as a fundamental right. It also underpins the challenges generated by the pervasive use of new information and communications technologies (ICTs) in today's digital society, which has enabled the collection and use of vast amounts of personal data with phenomenal ease and efficiency.

ICT innovations and applications such as the internet, social media, mobile applications and cloud computing have become ubiquitous. No doubt these technologies have created great economic and societal values, and enhance the productivity and competitiveness of enterprises in ways beyond our imagination.

At the same time, they also pose immense risks to privacy and raise serious concerns about the protection of personal data. For example, the memory of a USB drive today could be 64GB or more, bigger than that of a mini-computer 15 years ago. The inadvertent loss of a USB today containing 64GB of sensitive personal data could be disastrous.

### Minimalist Approach to Tackle Privacy Issues

Against this fast evolving privacy landscape, where do organisations in Hong Kong stand in terms of managing privacy and data protection? To say the least, there is definitely room for improvement.

In many of the complaint cases the Office of the Privacy Commissioner for Personal Data (PCPD) has investigated, we found that organisations tend to adopt a rather passive attitude. They were reactive instead of proactive and remedial instead of preventative. Privacy concerns were only addressed seriously when mistakes have been made and identified.

《個人資料(私隱)條例》(條例)於1996年實施,但多年來,私隱和個人資料保障依然是一門未受重視的課題。

公司和機構的日常管理,離不開處理財政預算、客戶服務、公共關係和人事管理等等。發展較成熟的機構為履行企業社會責任,會評估其業務運作對環境的影響;但反觀私隱和個人資料保障,在企業的議程上卻一直被置於較低的優先次序。處身「大數據」年代,顧客對私隱權有更高的期望,機構不可能再採用這種策略。

### 個人資料與私隱保障日益重要

香港是亞洲首個就個人資料私隱制訂專門法例的司法管轄區。時至今日,區內有十個司法管轄區已實施或即將實施類似的法例,包括南韓、澳門、越南、馬來西亞、日本、台灣、泰國、菲律賓、印度和新加坡。放眼全球,最少有102個司法管轄區已施行或將施行全面的個人資料保障法例。

此趨勢反映各地政府對私隱這項基本人權愈來愈肯定,亦回應了斬新資訊和通訊科技在現今的數碼化社會,大量個人資料可輕易及高效地被收集和使用的情况下所帶來的挑戰。

互聯網、社交網絡、物聯網、流動應用程式和雲端運算等資訊和通訊科技的創新和應用可謂無處不在,這些科技無疑超乎我們的想像,亦創造了巨大的經濟和社會價值,和提升機構的生產力和競爭力。

這些新科技同時亦帶來了重大的私隱風險,喚起大家嚴肅地關注對個人資料保障的影響。舉例說,一枚USB記憶體的容量可達64GB以上,比十五年前一部微型電腦的記憶體還要大。遺失載有敏感個人資料的USB記憶體,有可能帶來災難性的後果。

### 對私隱事宜採取可有可無的態度

私隱保障的大環境正經歷快速的演進,香港的企業和機構在管理個人資料和私隱方面應如何自處?最保守的答案是,肯定有改進空間。

個人資料私隱專員公署在調查投訴個案時發現,一些機構對待個人資料私隱流於被動,採取回應式和補救性的態度,多於主動處理和防範。惟有當機構犯錯而被公署發現時,私隱才受到關注。

最高管理層鮮有參與這方面的工作,有關事宜很多時交由法律和符規人員處理,這安排往往令機構在個人資料私隱保障方面採取可免則免的態度,止於符合條例規定的最低要求。

### 八達通事件

廣受公眾關注的2010年八達通事件是這方面的經典案例。公署發現該公司有二百四十萬會員的顧客忠誠計劃,在操作上違反了條例下多項規定。

Top management was seldom involved, if at all. The subject was delegated to the legal and compliance staff. This led to the adoption of a minimalist approach which was concerned with just meeting the legal requirements set out in the Ordinance.

### The Octopus Case

The Octopus incident of 2010 is a textbook example of this approach. In running its customer loyalty programme with a data base of 2.4 million subscribers, we found the company had committed a number of contraventions under the Ordinance.

In particular, without its customers' consent, it had transferred their personal data to a number of partner companies for use in the marketing of the latter's products and services. It received monetary gains from the partner companies in exchange for the data transfer. The transaction, in essence, was a sale of private personal data.

In response, Octopus' concluding remarks to the case, promulgated widely in a paid advertisement in the media, were as follows: "What it did has a legal basis but failed to meet the aspirations of the community".

I certainly disagree with Octopus' explanation of a "legal basis" but I am completely in support of its self-admission of failure to meet its customers' privacy expectation.

### Continued Privacy Violations

I expected that the Octopus case would serve as a wake-up call to many organisations. This is certainly the case insofar as the collection and use of personal data for direct marketing is concerned. The Ordinance was amended in 2012 to provide for, among other things, a set of highly regulated procedures the violation of which constitutes an offence that attracts heavy penalties.

However, our subsequent investigations indicated that other contraventions committed by Octopus had continued in the privacy practices of a significant number of major organisations.

One notable example was a repetition of the Octopus mistake of excessive collection of personal data, namely, collecting the customers' identity card numbers (and in some cases, copies of the identity cards) for member authentication, when other contact information already sufficed for that purpose. Organisations tend to collect personal data without giving serious thought to what real purposes the data collected could serve. Further, they tend to over-emphasise their administrative and operational convenience, at the expense of data subjects' privacy and data protection. When it comes to authentication, they tend to require the strongest level of authentication regardless of the nature of the transaction. Little regard seems to have been paid to the fact that identity card data is highly personal and sensitive and if it falls into the wrong hands, the affected persons could suffer from an enhanced risk of identity theft, administrative nuisance or financial loss.



該公司未經顧客同意而將顧客的個人資料轉交給多間業務夥伴公司，以供這些夥伴公司作促銷產品和服務之用，從中獲取夥伴公司的金錢利益。有關的資料轉移，根本上是出售市民的個人資料私隱。

八達通在總結該事件時，在傳媒大肆刊登了一則廣告，自言「今次出售客戶個人資料，雖然於法有據，但於情不合……」。

我對八達通當時提出的「法理依據」不敢苟同，但對於該公司承認做法未能迎合顧客的私隱期望，於情不合，我完全認同。

### 再三侵犯私隱

我預期該八達通事件會對很多機構產生警誡作用，在收集和使用個人資料作直接促銷用途方面的確如是。條例在2012年經過多項修訂，當中包括引入嚴格的規管程序，違者將面對相當重的刑罰。

然而，修例後我們在一些個案調查中依然看到有相當數目的大機構，在處理個人資料私隱方面重犯八達通其他違例的錯誤。

其中一個明顯的例子是，有機構重蹈八達通收集超乎適度個人資料的覆轍，收集顧客的身份證號碼（在一些個案中更涉及收集身份證副本）以作為核實客戶身份用途，而實際上其他聯絡資料已足以達致該目的。機構收集個人資料時傾向寧濫莫缺，而未有認真思考收集得的資料可達致的真正目的為何。再者，他們傾向過於著重行政和操作方便，而犧牲了客戶的私隱和

Another example was the continued use of the same vague terms that Octopus once adopted to define the third parties to whom the personal data collected would be transferred, such as “subsidiaries”, “partners”, “affiliates”, “third parties” and “any other persons under a duty of confidentiality to us”. These terms, for some obscure reasons, have been commonly used by many organisations in their privacy notices. But they gave no clue to the customers as to the nature of the business of the third parties. Customers could not therefore make an informed choice on whether or not to accept such data transfer.

In many of the investigations the Office of the PCPD has conducted, it appeared to us that only the organisation’s legal and compliance staff was involved. Despite the sheer blatancy of the privacy contraventions, they did not see the need to take some prompt remedial actions to salvage the predicament. In some cases, upon receipt of our determination that the organisation had contravened the Ordinance, their immediate reaction was to file an appeal with the Administrative Appeal Board. Only when the investigation report was published and the case was put in the glare of the public spotlight was there a change in the organisation’s attitude. Its senior management, who seemed to be alerted of the contravention for the first time, invariably reacted in a positive manner and very often decided to drop their appeal.

### From Compliance to Accountability

Organisations certainly need a systematic and professional approach to managing privacy and data protection. They have to come to grips with the fact that public awareness and understanding of individuals’ privacy rights concerning personal data has been growing and there is high expectation that these rights are respected. One indicator of the public’s growing concern about privacy is that in the past four years, our workload in terms of the number of complaints received has increased by 80%.

To manage privacy and data protection responsibly, organisations can no longer merely treat them as a legal compliance issue, perform the least possible to comply with the legal requirements, with little or no regard to customers’ privacy expectations. Organisations should adopt a proactive strategy that embraces personal data privacy protection as part of their corporate governance responsibilities and apply it as a top-down business imperative throughout the organisation. This calls for a paradigm shift from compliance to accountability and the formulation and maintenance of a comprehensive privacy management programme.

### Privacy Management Programme

A privacy management programme should be a robust privacy infrastructure that: –

- has top management commitment and is integrated into the organisation’s governance structure;
- treats privacy and data protection as a multi-disciplinary issue, (not merely as a legal compliance issue), with a special focus on respect for customers or clients’ needs, wants, rights and expectations;

個人資料保障。在核實身份方面，機構不顧交易的性質而傾向採用最嚴謹的核實程序，似乎未有仔細考慮身份證資料屬於高度個人化和敏感，假使落入不法之徒手中，受影響的當事人可能會被盜用身份、蒙受滋擾或經濟損失。

另一例子是在交代公司收集所得的個人資料會轉交給哪些第三方方面，一些機構沿用「附屬公司」、「夥伴」、「聯營公司」、「第三方」和「任何對我們負有保密責任的人士」等八達通曾採用的籠統字眼，基於種種費解的原因，這些用詞為機構普遍地寫在其私隱政策聲明中。但這些用詞根本沒有清楚說明第三方的業務性質，顧客難以就是否接受機構轉移其個人資料的做法作出知情決定。

我們也看到，機構一般只讓法律和符規人員參與協助我們的調查，儘管違規情況相當明顯，他們認為沒有需要採取即時的補救措施去糾正錯誤。在一個案中，機構在知悉公署斷定案件有違規情況後的即時反應是向行政上訴委員會提出上訴。直至調查報告發表，個案惹起公眾注視時，機構才有態度上的轉變。其管理高層人員似乎在那一刻才發現機構的違規情況，因而採取正面的反應，很多時會決定中止上訴。

### 由符規躍升為問責

機構顯然需要有系統和專業的方式去管理私隱和個人資料保障。它們必須明白公眾的私隱意識和對個人資料私隱權的認知與日俱增，社會對於這些權利受到尊重的期望相當高。過去四年，公署接獲侵犯私隱投訴的數字增加了八成之多，正反映公眾關注的提升。

機構要負責任地管理私隱和個人資料保障，便不能僅視之為遵從法規的事宜，為求符規而私隱保障的工作採取可免則免的態度，妄顧顧客的私隱期望。機構應採取進取的策略，把個人資料私隱納入為企業管理責任的一部分，並在機構裡由上而下地貫徹執行這項業務不可或缺的一環。機構需要在策略上由符規躍升為問責，建立和維持全面的私隱管理系統。

### 私隱管理系統

私隱管理系統必須建基於：


- 機構最高管理層的決心和支持：由上而下推動，並且納入機構的管治架構內；
- 視私隱和資料保障為跨部門的事宜，而不僅是遵從法例的事，專注於尊重顧客和客戶的需要、要求、權利和期望；
- 制訂政策和程序，以確保機構遵從《個人資料（私隱）條例》的要求；
- 進行私隱風險評估以識辨潛在的私隱風險，採取措施減低風險；
- 確保私隱保障貫徹於所有新舊項目和服務的設計中；
- 為可能發生的個人資料外洩或私隱事故制訂應變機制；

- establishes policies, procedures and practices giving effect to the legal requirements under the Ordinance;
- provides for appropriate safeguards based on privacy risk assessment;
- ensures that privacy is built by design into all initiatives, programmes or services;
- includes plans for responding to breach and incident;
- incorporates internal oversight and review mechanisms;
- is kept current and relevant, and remains practical and effective in a rapidly changing privacy ecosystem; and
- is appropriately resourced and managed by dedicated staff.



- 設置內部監察及檢討機制；
- 能夠有效地回應私隱生態系統的迅速變化，保持實用，合事宜和相關；
- 有適當的資料配合和專責人員管理。


Apart from ensuring legal compliance, the implementation of a privacy management programme will demonstrate an organisation's commitment to good corporate governance and is conducive to building trustful relationships with customers, employees, shareholders and regulators. It is gratifying to note that Octopus has been adopting this accountability approach in the aftermath of the 2010 contraventions.

Organisations interested in developing and maintaining a privacy management programme may check our guidance at [www.pcpd.org.hk/pmp](http://www.pcpd.org.hk/pmp). 

— Allan Chiang

Privacy Commissioner for Personal Data

除了確保遵從法例要求，推行私隱管理系統可展示機構實踐良好企業管治的決心，而且有助建立與客戶、員工、股東和規管者之間的互信關係。值得可喜的是，八達通在發生2010年的違規事件後已採納這種問責的方式去處理客戶的個人資料。

機構如有意建立和推行私隱管理系統，可登入 [www.pcpd.org.hk/pmp](http://www.pcpd.org.hk/pmp) 參閱我們發出的指引。 

— 蔣任宏

個人資料私隱專員

# Making Business Sense

Targeting Your Customers for MAXIMUM Results



For Advertising in Momentum, the official publication of CHKLC, please contact:

**ninehills**  
media

**Clariss Tam**  
T: +852 3796 3060  
E: [claris@ninehillsmmedia.com](mailto:claris@ninehillsmmedia.com)

**CHKLC**  
香港上市公司協會  
THE CHAMBER OF HONG KONG LISTED COMPANIES

**Amy Leung**  
T: +852 2970 0886  
E: [amyleung@chkcl.org](mailto:amyleung@chkcl.org)