Implementing a Privacy Management Programme to Gain Customers' Trust

實施私隱管理系統　贏取客戶信任

Ada CHUNG Lai-ling 鍾麗玲

In the words of Jack Ma, "We collect data from selling things. Data is the most valuable asset of Alibaba (我們是通過賣東西收集數據，數據是阿里最值錢的財富)."

With the exponential growth of digitalisation in the past decade, the collection and use of personal data has become of unprecedented importance for most businesses, especially those who provide online services and products. Other than requesting greater transparency, customers nowadays expect companies to clearly inform them of how their personal data, once collected, will be used and for what purpose. It is self-evident that the importance and priority that a company places on the handling of personal data privacy directly affects the confidence and trust that customers have in the company and, in turn, the competitive edge of the company.

Against this background, my office, the Office of the Privacy Commissioner for Personal Data, Hong Kong (PCPD), advocates that **companies should develop their own Privacy Management Programme (PMP) and appoint a Data Protection Officer** in order to institutionalise a proper system for the responsible use of personal data that is in compliance with the Personal Data (Privacy) Ordinance (the Ordinance), Cap. 486 of Laws of Hong Kong. Starting from the boardroom, companies should embrace personal data protection as part of their corporate policies and culture, and apply it as a business imperative throughout the companies. A PMP can help companies gain trust from customers and other stakeholders. With trust garnered, companies will be rewarded with loyalty from their customers and business partners, which is all the more important in a fast-changing business environment.

Directors have a unique and pivotal role in implementing the PMP as an essential part of their companies' commitment to good corporate governance. Implementing a PMP involves fostering a culture of respecting and protecting personal data privacy, which cannot be made possible without the steer and leadership of the directors. **Indeed, in the Guide for Independent Non-Executive Directors newly published by The Hong Kong Institute of Directors, companies are encouraged to implement a PMP as one of the drivers for the adoption of "Environmental, Social and Governance" (ESG) management.**

Benefits of implementing a PMP

Characterised by the accountability principle, a PMP is a management framework for the responsible collection, holding, processing, and use of personal data. With a PMP in place, companies can:

- minimise the risks of incidents in relation to data security;

- handle privacy breaches effectively with established procedures and protocol to minimise the damage arising from those breaches;
- manage collected personal data effectively;
- ensure compliance with the Ordinance;
- demonstrate the companies' commitment to good corporate governance and building trust with customers and relevant stakeholders; and
- enhance corporate reputation, competitive advantage and potential business opportunities.

What are the components of a PMP?

A comprehensive PMP requires companies to adopt a top-down approach, strengthen staff awareness of data privacy protection, and devise policies and procedures in relation to collection, holding, processing and use of personal data so as to ensure compliance with the Ordinance, including the Data Protection Principles specified in the Ordinance.

A PMP should consist of the following three sets of components at the minimum:

1. Organisational Commitment
   - Buy-in from the Top
   - Appointment of Data Protection Officer / Establishment of a Data Protection Office
   - Establishment of Reporting Mechanism

2. Programme Controls
   - Personal Data Inventory with information on the kinds of personal data the company holds and how the personal data is processed
   - Internal Policies on Personal Data Handling
   - Risk Assessment Tools
   - Training, Education and Promotion
   - Handling of Data Breach Incident
   - Data Processor Management
   - Communication with employees, customers and stakeholders

3. Ongoing Assessment and Revision
   - Development of an Oversight and Review Plan
   - Assessment and Revision of Programme Controls

Establishing organisational commitment is vital to PMP

"Organisational commitment", as a key component of PMP, is of particular relevance and importance to directors, as directors are effectively the stewards for promoting the success and good governance of their companies, including data accountability. This key component of the PMP will be explained in more detail below.

Buy-in from the Top

To enhance accountability, a top-down approach is necessary for companies to demonstrate their commitment to fostering a respectful culture for privacy and determination to protect personal data privacy. Under the stewardship of directors, the PCPD recommends that, the top management should:

- convey to all staff their support to cultivate a respectful culture for personal data privacy and commitment to the implementation of PMP through staff meetings or internal circulars;
- appoint a Data Protection Officer;
- endorse the programme controls and the whole PMP;
- allocate adequate resources, including but not limited to finance and manpower, to implement PMP;
- actively participate in the assessment and review of PMP; and
- report the progress of the implementation of the programme to the Board of Directors regularly.

It is recommended that directors work with the management to ensure resiliency strategy and data protection infrastructure are in place, and that internal policies and procedures on the protection of personal data are followed.

Appointment of Data Protection Officer / Establishment of a Data Protection Office

The PCPD recommends that companies appoint a designated officer as the Data Protection Officer to oversee the companies' compliance with the Ordinance and implementation of the PMP. For a large corporation, the Data Protection Officer should be a senior executive, whereas for a small business, this can be the owner or manager.

The Data Protection Officer is responsible for structuring, designing and managing the PMP, which involves all relevant procedures, training, monitoring or auditing, documenting, evaluating, and other follow-up actions in relation to the collection, holding, processing and use of personal data. In large corporations, understandably more personal data is collected and used by various departments and business units. It is therefore recommended that departmental coordinators be appointed to support the Data Protection Officer. Resources should be channelled to train

and develop the Data Protection Officer as a professional in the protection of personal data privacy.

Establishment of Reporting Mechanisms

Reporting mechanisms are indispensable for oversight by the Board. In this regard, companies should establish internal reporting mechanisms, stating clearly the structure and procedures for reporting the overall compliance situation, the problems encountered, the complaints in relation to personal data privacy received and incidents of possible data breaches. Other than regular reports, the management should also provide exceptional reports on major risks and anomalies to the Board of Directors.

An effective reporting mechanism would be imperative at times when escalation of personal data issues is needed, such as when a major data breach takes place or a large number of complaints relating to data privacy are received. The mechanism would also help determine who should be involved, their respective responsibilities and where the ultimate decisions should be made. These personnel could be representatives from technical, operational, legal and corporate communications streams. To successfully implement the reporting mechanism as one of the key attributes of the PMP, how and when to escalate should be clearly defined and explained to employees. Companies should also document all of their reporting procedures.

Conclusion

With the ever-rising expectation of customers and stakeholders on the responsible use of personal data by companies, companies should not stop at just ticking the box. The protection of personal data privacy should no longer be seen and merely managed as a compliance issue. After all, doing the least to comply with the legal requirements is not the cure nor the global trend anymore. Instead, companies should also observe good data ethics and should consider the subject from a broader perspective, bringing the concept of customer centricity into the business equation. The commitment of directors and the management is paramount in building and maintaining a PMP so as to ensure that privacy is built in by design in initiatives, programmes or services, and data protection is practised throughout the company. Such a proactive approach would lead to a win-win outcome for companies, their customers as well as other stakeholders.

For examples and practical guidance on how to devise and implement a comprehensive PMP, please refer to the *Best Practice Guide on Privacy Management Programme* issued by the PCPD.

Ms Ada CHUNG Lai-ling is a Barrister and Privacy Commissioner for Personal Data, Hong Kong. She is also Hon Fellow of HKIoD.

馬雲曾經說過：「我們是通過賣東西收集數據，數據是阿里最值錢的財富」。

隨著近年數碼化發展迅速，收集和使用個人資料對不同業界變得至關重要，特別是提供網上產品及服務的企業。企業對個人資料私隱的重視程度，會直接影響客戶的信心和信任，以至企業的競爭優勢。

作為香港個人資料私隱專員，**我提倡企業應設立私隱管理系統，並委任保障資料主任**，以建立一套遵從香港法例第486章《個人資料（私隱） 條例》（《私隱條例》）規定的制度，循規地使用個人資料。私隱管理系統有助企業贏得客戶及其他持份者的信任，從而不會被客戶及業務伙伴所離棄。**董事在實施私隱管理系統上擔任獨特而關鍵的角色。香港董事學會最新出版的《獨立非執行董事指南》，便鼓勵企業實施私隱管理系統，作為實踐「環境、社會及管治」管理的其中一環。**

私隱管理系統的主要部分

私隱管理系統有以下三個主要部分：

1. 機構的決心
2. 系統管控措施（例如個人資料庫存、處理個人資料的內部政策）
3. 持續評估及修訂（例如制定監督及檢討計劃）

在各主要部分中，「機構的決心」與董事的角色息息相關，對董事亦至為重要，因為董事是帶領企業邁向成功及良好管治的舵手。為加強問責，企業應由上而下去締造尊重及保障個人資料私隱的文化。董事應與管理層合力確保企業訂立應變策略及保障資料的架構，以及貫徹執行保障個人資料的政策和程序。

我亦建議企業委任保障資料主任，以監督企業遵從《私隱條例》的規定及落實推行私隱管理系統。企業應投入資源，培訓保障資料主任成為保障個人資料私隱的專才。

匯報機制對董事會的監督亦不可或缺。企業應建立內部匯報機制，訂明執行及管理私隱管理系統的負責人，報告企業整體的循規情況等。當有需要將個人資料事故提升至更高的層面處理時，例如發生大型資料外洩事故或接獲大量資料私隱相關的投訴，有效的匯報機制就可發揮重要作用。

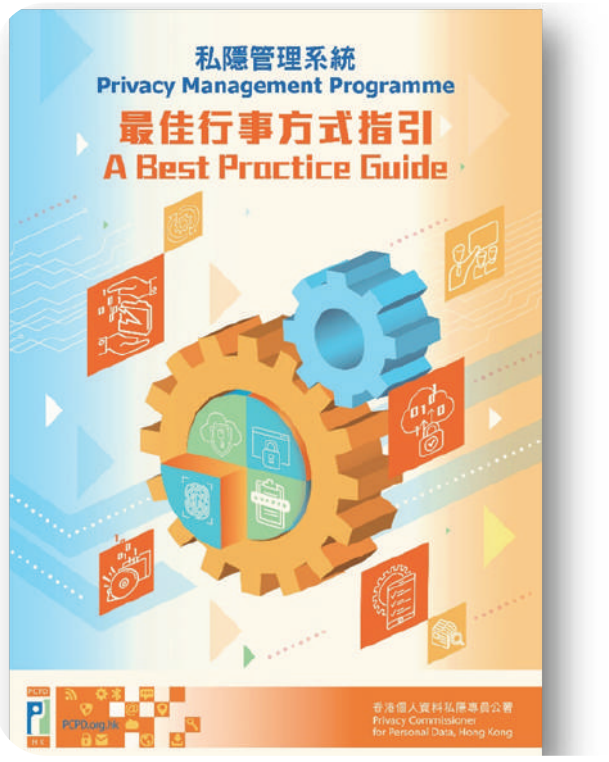
結語

因應客戶與持份者對企業負責任地使用個人資料日益趨增的期望，企業不應把個人資料

私隱保障僅視為循規的要求。事實上，單單符合法例規定行事，已不再是解決方案，與全球恪守良好數據道德的趨勢亦不符。要成功設立並推行私隱管理系統，必須有董事會與最高管理層的支持，方能為企業、客戶和持份者帶來多贏的局面。

欲知道更多有關私隱管理系統的資料，請參閱香港個人資料私隱專員公署發出的《私隱管理系統 — 最佳行事方式指引》。

鍾麗玲大律師是香港個人資料私隱專員，亦是香港董事學會的榮譽資深會員。



▲ **Best Practice Guide on Privacy Management Programme issued by the Office of the Privacy Commissioner for Personal Data, Hong Kong**
香港個人資料私隱專員公署發出的《私隱管理系統 — 最佳行事方式指引》

The 21st Century DIRECTOR 廿一世紀董事

Sponsored by 贊助機構：
Corporate Governance Development Foundation Fund
企業管治發展基金

Publisher 出版機構
The Hong Kong Institute of Directors 香港董事學會

Sponsor 贊助機構
Corporate Governance Development Foundation Fund 企業管治發展基金

Publishing Board 出版委員會
Mr Stanley Mok (Chairman) 莫兆光先生（主席）
Ms Bonnie S Y Chan 陳心愉女士
Ms Agnes K Y Tai 戴潔瑩女士
Mr Richard Tsang 曾立基先生
Dr Carlye Tsui 徐尉玲博士

Project Management 項目統籌
Executive Office, The Hong Kong Institute of Directors
香港董事學會行政處

For enquiries about circulation and advertisement, please contact:
有關發行及廣告查詢，請聯絡：
Chief Business Officer: Ms Miriam Yee
業務總監：余海恩小姐

For editorial enquiries, please contact:
有關編輯上的查詢，請聯絡：
Associate Manager, Communication & Projects: Ms Joanne Yam
傳訊及項目副經理：任綺欣小姐

Tel 電話： +852 2889 1414
Fax 傳真： +852 2889 9982
Email 電郵： magazine@hkiod.com

《廿一世紀董事》同時可於網上閱覽
The 21st Century Director is also available at
http://www.hkiod.com/21century.html

ISSN 1996-9619

The Hong Kong Institute of Directors is Hong Kong's premier body representing directors to foster the long-term success of companies through advocacy and standards-setting in corporate governance and professional development for directors.
香港董事學會為香港代表專業董事的首要組織，其宗旨是促進所有公司的持久成就；為達成使命，學會致力提倡優秀企業管治與釐訂相關標準，以及協助董事的專業發展。

The Hong Kong Institute of Directors Executive Office 香港董事學會行政處
2104 Shanghai Industrial Investment Building, 48 Hennessy Road, Wan Chai, Hong Kong 香港灣仔軒尼詩道48號上海實業大廈2104
Tel 電話 : (852) 2889 9986 Fax 傳真 : (852) 2889 9982 E-mail 電郵 : executive@hkiod.com
The Hong Kong Institute of Directors 香港董事學會 The Hong Kong Institute of Directors