CSj

June 2014

Chartered Secretaries.
More than meets the eye.

特許秘書.潛能.超越所見.

The journal of The Hong Kong Institute of Chartered Secretaries

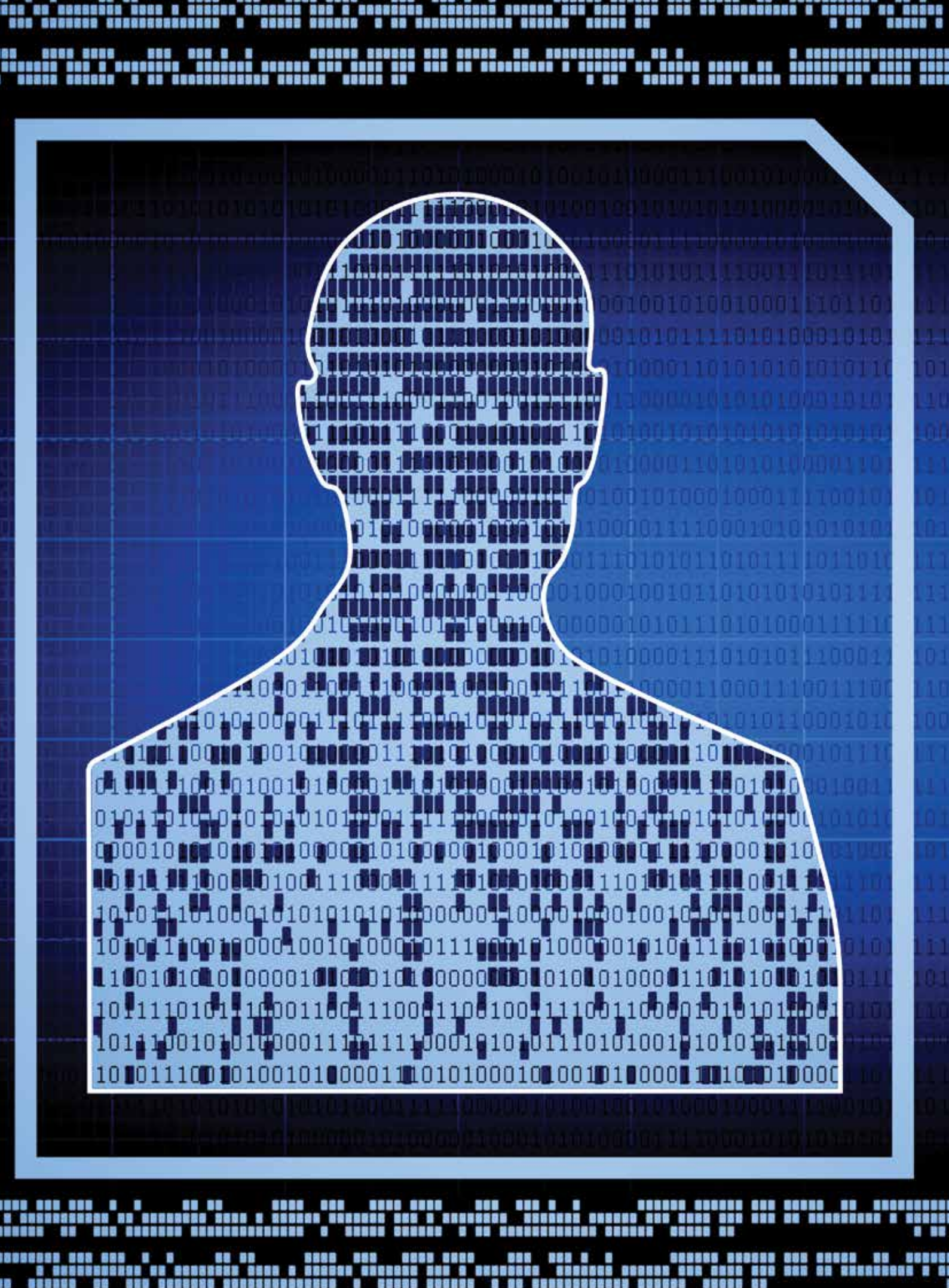
香港特許秘書公會會刊

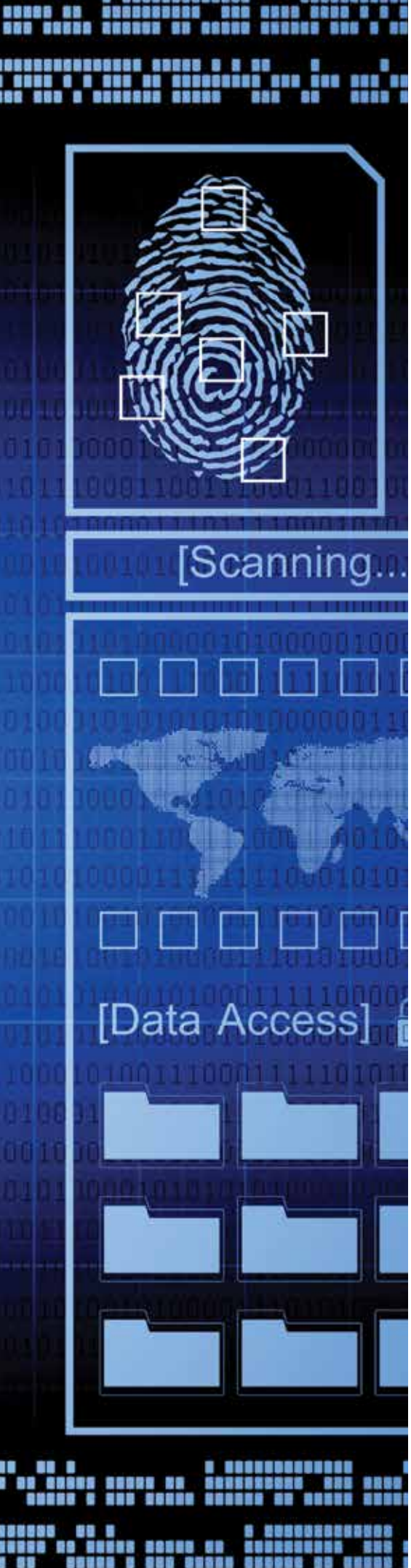
The ESG challenge

How to prepare a business review

Privacy compliance
CSIA Toolkit
INEDs in the PRC

65 CHARTERED SECRETARIES 特許秘書 Years in Hong Kong





Privacy and data protection: from compliance to accountability

Allan Chiang, Hong Kong's Privacy Commissioner for Personal Data, outlines the competitive benefits to be gained by adopting a comprehensive privacy management programme.

The Personal Data (Privacy) Ordinance (the Privacy Ordinance) came into force 18 years ago in 1996. At that time, Hong Kong was the first jurisdiction in Asia to have a dedicated piece of legislation on personal data privacy. As of today, 10 other jurisdictions in the region have similar laws in force or about to be in force. These are South Korea, Macau, 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 human 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.

Highlights

- companies often adopt a minimalist approach which is concerned with just meeting the legal requirements set out in the Privacy Ordinance
- establishing and maintaining a privacy management programme will demonstrate an organisation's commitment to good corporate governance
- in addition to ensuring legal compliance, a privacy management programme can build better relationships with customers, employees, shareholders and regulators

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.

Against this privacy landscape, public awareness and understanding of individuals' privacy rights concerning personal data has been growing at an accelerating rate. This has been associated with a series of high-profile privacy intrusion events. In particular, the landmark case of privacy contravention by the Octopus group of companies in 2010 has heightened public and media sensitivity and scrutiny over privacy issues.

Meanwhile, a survey conducted by Unisys Security Index in 2012 revealed that over 80% of Hong Kong people surveyed indicated that they were 'very concerned' or 'extremely concerned' about unauthorised access to, or misuse of, their personal data.

Another 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%.

Further, the Snowden affair last year has resulted in a public outcry over privacy on a global basis. Indeed 'privacy' was Dictionary.com's word of the year for 2013.

Room for improvement in managing privacy issues

Now, in this age of 'big data' and the unprecedentedly high level of customer expectations for their privacy rights, where do organisations in Hong Kong stand in terms of managing privacy and data protection? To say the least, this subject has been accorded a low priority in organisations' business agendas and there is definitely room for improvement.

In many of the complaint cases we have 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 had been made and identified.

Learning points in investigation reports went unheeded

We publish from time to time reports of investigations explaining in detail the privacy contraventions in question, our application of the Privacy Ordinance in determining the contraventions, and the remedies. This practice is intended to encourage compliant behaviour by not just the organisation being the subject of investigation but also other organisations facing similar privacy issues. We hope that every investigation report we issue will prompt many organisations to review their relevant privacy policies and practices with a view to seeking appropriate remedies or improvements. But not infrequently, this proves to be wishful thinking.

For example, one major learning point from the investigation report on the Octopus case is that organisations should not too readily collect from their customers highly sensitive personal data such as those contained in the Hong Kong identity card for authentication purposes which can be met by the supply of other less sensitive personal data. However, recent cases indicate that many organisations continue to over-emphasise their administrative and operational convenience, at the expense of their customers' privacy and data protection. They tend to require a strong level of authentication irrespective 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.

Another major learning point from the Octopus report is that organisations should use clear and specific terms to explain the purpose of use of the data they collect and the class of persons that the data may be transferred to. However, we found again from recent cases that many organisations, including some reputable brands, continue to use the same vague terms that Octopus once adopted to define the third parties that the data could be transferred to, 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 give no clue to the customers as to the nature of the business of the third parties. Customers may therefore be unable to make an informed choice on whether or not to accept such data transfer.

In December 2011, we published a report of an investigation against Hang Seng Bank with the determination that it was a contravention for them to retain customers' bankruptcy data for as long as 99 years. Since a bankrupt will normally be discharged upon expiry of a

> people are waking up to the value of their personal data, and companies which fail to handle people's information properly will lose their trust and even their business

period between four to eight years from the commencement of the bankruptcy, I concluded that the bankruptcy data should not be kept for more than eight years. In the report, I expressed the hope that other financial institutions engaging in similar practices would conduct reviews of their data retention policies to ensure they would not repeat Hang Seng Bank's mistake.

As it later transpired, some major banks continued to keep their customers' bankruptcy data well beyond eight years despite my intervention. They corrected the practice only when I threatened to take enforcement action.

Beyond legal compliance

On matters of privacy and data protection, it is not uncommon that top management is seldom involved, if at all. The subject is delegated to the legal and compliance staff. This often leads to the adoption of a minimalist approach which is concerned with just meeting the legal requirements set out in the Privacy Ordinance.
The infamous Octopus incident of 2010 again serves to illustrate this point. In running its customer loyalty programme with a database of 2.4 million subscribers, we found the company had committed a very serious contravention, namely, the transfer of the customers' personal data without their consent 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 that its conduct did have a legal basis but it failed to meet the aspirations of the community (于法有据; 但于情不合). I certainly disagree with Octopus' legal arguments but I am glad the company has realised that it should consider the issue beyond the bounds of the law.

Another case worth mentioning concerns a determination I made in 2012 on the complaints by three TV artistes against two gossip magazines, namely, *Sudden Weekly* and *Face Magazine*. They concerned the use of systematic surveillance and telescopic lens photography to take clandestine photographs of the artistes' daily lives and intimate acts within their private residences over a period of three to four days. These photos, including one showing one of the complainants in an undressed state, were published in the magazines.

I ruled that in the circumstances, taking of the photos surreptitiously amounted to unfair collection of personal data, and directed the magazines to delete the photos from their database and websites, and to establish privacy guidelines for compliance by their staff on the systematic monitoring of the collection of personal data by covert means and/ or long-distance photography.

This determination has been vehemently challenged by the two magazines. They lodged an appeal with the Administrative Appeal Board and failed. They are now seeking a judicial review of the decision of the Administrative Appeal Board. Their arguments are all legalistic, concerning the interpretation of the law, for example, whether I have the legal authority to require them to formulate privacy guidelines for compliance by their staff.

I doubt whether the privacy issues in question should be handled by the magazines merely as a strict legal dispute. Irrespective of whether I have the legal authority to require them to formulate privacy guidelines for compliance by their staff, as responsible employers and news organisations, shouldn't they do it anyway?

From compliance to accountability: adopting a privacy management programme

I submit that we need to consider privacy from a broader management perspective and take into account factors such as corporate reputation and respect for the basic rights of the customers or clients. As responsible corporate citizens, organisations have to proactively embrace personal data privacy protection as part of their corporate governance responsibilities and apply it as a top-down business imperative throughout the organisation.

These all call for a paradigm shift from compliance to accountability and the formulation and maintenance of a comprehensive privacy management programme (PMP).

As promulgated in our *Privacy Management Programme: A Best Practice Guide*, a PMP 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 multidisciplinary issue (not merely as a legal compliance issue), with a special focus on respect for customers' or clients' needs, wants, rights and expectations
- establishes policies, procedures and practices giving effect to the legal requirements under the Privacy 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 breaches and incidents
- incorporates internal oversight and review mechanisms
- is kept current and relevant, and remains practical and effective in a rapidly changing privacy environment, and
- is appropriately resourced and managed by dedicated staff.

Apart from ensuring legal compliance, establishing and maintaining a PMP will demonstrate an organisation's commitment to good corporate governance and is conducive to building trustful relationships with customers or citizens, employees, shareholders and regulators.

Privacy protection as a competitive advantage

Indeed, building and maintaining customers' trust is the cornerstone of a business' competitive advantage. People are waking up to the value of their personal data, and companies which fail to handle people's information properly will lose their trust and even their business. For this reason, many leading companies are proactively adopting privacy-friendly business practices.

In this regard, it is interesting to watch Microsoft's recent campaign against Google for reading each and every word of the email messages of Gmail users and serving up ads based on the content of these messages. At the same time, this software giant is encouraging people to use Hotmail which reportedly dose not go through emails to sell ads.

In a similar vein, we note Yahoo's recent announcement that it had implemented a series of stronger security and privacy measures, including securing traffic that moves between its servers and encrypting most search queries automatically. This has been dogged by critics as a strategy to catch up with its competitors in safeguarding the security of its email delivery systems. For example, the Edward Snowden revelations about the US National Security Agency reportedly showed that the agency was collecting substantially more addresses of webmail users from Yahoo than Hotmail or Gmail.

In Hong Kong, it is very encouraging to witness that all the government bureaus and departments, together with 25 companies from the insurance sector, nine companies from the telecommunications sector and five organisations from other sectors, have pledged to adopt a PMP. It is particularly gratifying to note that Octopus is on the pledge list, as it has been adopting this accountability approach in the aftermath of the 2010 contraventions.

Allan Chiang
Privacy Commissioner for Personal Data