Managing a breach of security in the public sector

Ashley Roughton, Barrister, Chambers of Dr Ashley Roughton

This Practice Note has been taken from Lexis® Practical Guidance Hong Kong – Data Protection

This Practice Note sets out actions to be taken upon a security breach and measures to avoid further risks.

As the way we work continues to evolve from wireless connections, mobile computing and cloud computing to tablets and smart phones, the associated risk to personal data carried on these devices, and in these places, also evolves. Understanding this ever-changing landscape of risk and putting effective safeguards in place is a process that is particularly pertinent in the public sector.

Since public sector organisations often dealing with vast amounts of data, in many cases with financial and national security implications never far away, public sector bodies have an acute responsibility in managing breaches of security in relation to data.

The Personal Data (Privacy) Ordinance (Cap 486) (PDPO) provides that the personal data of data subjects in Hong Kong must be protected and processed lawfully by data users. It requires data users to implement appropriate security measures to ensure protection.

Principle 4 of Schedule 1 to the PDPO notes that:

'Principle 4 – security of personal data

(1) All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing, erasure, loss or use having particular regard to:
  (a) the kind of data and the harm that could result if any of those things should occur;
  (b) the physical location where the data is stored;
  (c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;
  (d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and
  (e) any measures taken for ensuring the secure transmission of the data.

(2) Without limiting subsection (1), if a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

(3) In subsection (2):

data processor has the same meaning given by subsection (4) of data protection principle 2.'

This principle has three important aspects, which a data user should take note of:

- the prevention of unauthorised and accidental (though apparently not unlawful) activity
- that the activity is access, processing, erasure, loss or use
- passing on the Data Protection Principle 4 to processors (whether within or outside Hong Kong) by contractual means

Privacy Commissioner for Personal Data (PCPD) is the regulatory body for data protection in Hong Kong. In the event of a breach occurring, the PCPD has the authority to take action (though it cannot impose fines or monetary penalty notices).

Managing a breach

If a public sector organisation discovers that there has been a security breach, there are a number of key steps that the organisation should take in order to manage the situation as efficiently as possible:

- investigation – as part of the immediate response and recovery process, an investigation into why the breach took place and the nature of the breach is required. The investigation will provide the organisation with an understanding of:

    - the extent of the breach
    - the damage already caused and the damage that may potentially be caused to the data subject(s)
    - the course of action that is most suitable in containing the breach and/or preventing a further breach

- stop/mitigate the breach – with an understanding of the breach and its cause, the organisation can then take appropriate action to mitigate the effects of the breach and prevent the breach from continuing and/or recurring (if possible). Such action may involve a combination of notification, contractual, disciplinary and procedural steps. Where the PCPD carries out an investigation, it will require information in relation to how the breach was stopped or mitigated and also how the organisation will prevent future breaches of a similar nature from occurring in accordance with the organisation's Principle 4 obligations

- notification – the organisation will have to consider who should be notified of the breach. This is an important process in containing, managing and reviewing the breach. Depending upon the detail and scale of the breach, there are a number of parties who may need to be informed of the breach:

    - PCPD – while there is no express requirement in the PDPO, PCPD's Guidance on Data Breach Handling and the Giving of Breach Notifications suggests that a 'serious breach' be notified to them

    - insurers – an organisation should check all relevant insurance policies, which may include terms that require the organisation to notify its insurers of any breach

    - other data controllers – an organisation is not legally obliged to do so, but where other data controllers might be responsible for data affected by the breach, then it is considered good practice to notify them

    - data subjects – data subjects are not required to be notified of a data security breach unless a reason exists for doing so. This may include where the data subject would benefit from knowing, ie they can perhaps change a password or account settings

    - other relevant organisations – depending on the nature of the breach, the public body may require external assistance from specialist IT companies and in most cases will be required to make a report to the police

    - information and external relations management – this is key; make sure that you have PR specialists available and as pre-briefed as possible. The adverse consequences of many a breach have been avoided by careful PR

- contractual obligations – if the data protection breach occurred due to the fault of a data processor, then the organisation should review the contractual obligations between the parties and assess whether there is a potential claim for liability or whether the contract can be terminated due to the breach, or if the public body does not wish to proceed to terminate, what further technical measures require to be implemented by the data processo

- disciplinary action – in the event that the organisation identifies one or more of its employees as being at fault or clearly responsible for the breach, the organisation should consult its own constitution, relevant procedures and policies prior to initiating any disciplinary process. In particular, it should consider the background of the employee or party responsible, and whether adequate training and guidance had been provided beforehand

- procedural review – finally an organisation should evaluate whether it has appropriate data security policies and procedures. If so, it should establish whether these policies and procedures were correctly followed. If not, then the organisation should consider what action is

Security breach team

In navigating the challenges presented by a data security breach a security breach team should be put in place to deal with any incidents. With appropriate training, an understanding of individual and collective responsibility, and senior officer involvement, a security breach team may be best placed to effectively oversee and action the key steps in managing the breach.

Practical context

While no such issues have arisen and no reports have been forthcoming in Hong Kong in June 2014, the UK Information Commissioner highlighted some of the key data protection issues faced by British social housing organisations, following the UK Information Commissioner's Office (ICO) report which was published in February 2014. This report addressed 20 challenges that social housing organisations face such as data sharing, remote working, training, staff awareness, various IT and privacy policies and security. The report yields important insight into the general issues at play in a public sector environment. Various types of security issue were highlighted in the report, such as physical security at an organisation's premises, printing security and password security.

One of the ICO's suggestions related to limiting employee access to certain areas in the relevant premises. This could be by way of a swipe card, which only gives certain employees access to areas where personal data were stored and were accessible. If employees do not require access to all areas of premises, this may be particularly effective.

If organisations allow remote working, then it would be beneficial to have policies in place which address how this can be carried out safely and when it is appropriate. Certain types of home working could involve employees carrying around large volumes of personal data in paper or (easily losable) electronic form. Employees should be fully aware of their responsibilities in relation to home or remote working.

The challenges facing social housing organisations gives practical context to the prescribed procedure and can be extrapolated to any number of public sector bodies, given the similarity in procedure across the various sectors.

Minimising further risk

Public bodies can proactively manage the risk of security breaches occurring by ensuring organisation-wide awareness of security principle compliance considerations. By having a framework of policies and procedures, aligned with adherence to good practice, public bodies can limit exposure as far as practically possible. Basic safeguards for any public body should include:

- policies – including a Data Protection Policy, IT and Internet Use Policy, Data Retention and Destruction Policy, Data Security Breach Management Policy, Remote Working Policy and Social Media Use Policy

- processes – including IT and security controls, security level categorisation for personal data, training and education, and

- contract vetting – including vetting data processors, using the model services contract, data processor contracts, reporting, audit and correction, staff vetting, confidentiality, liability clauses and indemnities, security breach reporting, remediation and termination procedure

About the author

Ashley Roughton, Barrister, Chambers of Dr Ashley Roughton, is a Graduate chemist and master's level economist in competition and regulation, with a PhD in applied mathematics and engineering. He is author of the two standard and top recognised texts in patents and trade marks, and has over 24 years litigation experience as well as a strong transactional practice. Ashley is regularly cited as the top Data Protection and a top Intellectual Property lawyer in the UK.

Ashley is an author for Lexis® Practical Guidance Hong Kong – Data Protection, a one stop solution for all your data privacy needs.

LexisNexis®