VIVIEN CHAN & CO.
YOUR GREATER CHINA LAWYERS
HONG KONG | BEIJING

NEWSLETTER
issue 20 . 2018

IP UPDATE

Anna Mae Koo PARTNER
MA (Law) (Hons), University of Cambridge (Prince Philip Scholar)

- Asialaw Rising Star Lawyer in Intellectual Property 2018
- Techstars Mentor 2015
- IP Rising Star (Euromoney Women in Business Law Awards) 2013
- Litigation Committee Member, International Bar Association
- Anti-Counterfeiting Committee (2018), Internet Committee (2014-2016), INTA

Martin Lo ASSOCIATE
BSc (Hong Kong University of Science and Technology)
JD (Chinese University of Hong Kong)

Arthur Chan ASSOCIATE
BA (University of Leicester)
JD (Chinese University of Hong Kong)

Data Breach: What to Know, How to Prevent and How to Handle

I. BACKGROUND

This year, globally and in Hong Kong, there have been a number of high-profile personal data security breach incidents. In March, 50 million Facebook profiles globally were harvested by a data analytical firm, Cambridge Analytica. In April, the personal data of around 380,000 customers of the Hong Kong Broadband Network ("HKBN") were compromised in a cyberattack. In October, Hong Kong flag carrier Cathay Pacific announced that personal information of up to 9.4 million passengers has been leaked, including information such as passport numbers, credit card numbers, nationalities, phone numbers, etc. In late November, a consumer credit reporting agency, TransUnion, was found to be able to easily obtain the credit reports for a number of high-profile public figures, including Chief Executive Lam Cheng Yuet-ngor and Financial Secretary Paul Chan Mo-po due to TransUnion's simple online authentication procedures, and TransUnion was demanded to immediately suspend its online credit report services. What's more, last week, personal data of up to half a billion guests of Marriott International, one of the largest hotel groups globally with over 6000 hotels in 127 countries, has reportedly been exposed in one of the most serious data breaches in recent years.

The recent proliferation of such data breach incidents is indeed a wake-up call for data users, i.e. a legal entity or a person who controls the collection, holding, processing or use of the data. Data users should have a basic understanding of the statutory requirements on the protection of personal data and take out necessary actions to comply with such requirements.

In this article, we will set out the basic legal principles regarding the data protection regime in Hong Kong and our tips on how to prevent data breaches and how to respond in a data breach crisis.

II. THE PERSONAL DATA (PRIVACY) ORDINANCE

In Hong Kong, laws on data protection are generally governed by the Personal Data (Privacy) Ordinance (Cap. 486 of the Laws of Hong Kong) (the "PDPO"), which regulates the collection, use and handling of personal data and is based on a set of six data protection principles, which are widely adopted across many jurisdictions, namely: -

(i) Data Collection Principle – data should be collected for a lawful purpose and no more than necessary, and data subjects must be notified of the purpose and the classes of persons to whom the data may be transferred;

(ii) Accuracy & Retention Principle – data should be accurate and not be retained longer than necessary;

(iii) Data Use Principle – data should be used for the purpose for which the data is collected or for a purpose to which the data subject has consented;

(iv) Data Security Principle – data users should take practicable steps to safeguard personal data;

(v) Openness Principle – data users' personal data policies and practices should be made known to the public; and

(vi) Data Access & Correction Principle – the data subject is entitled to access and correct his/her data.

In the context of breach, the security of personal data is of utmost importance. According to the Data Security Principle, a data user must take all practicable steps to ensure that personal data is protected from unauthorized or accidental access, processing, erasure, loss or use. Generally, factors taken into account when determining what constitutes practicable steps include measures concerning the physical location and equipment where the data is stored, persons who have access to the date, and secure transmission of the data. These three are important measures that a data user must carefully devise, as they are ultimately common sources of data breaches.

Under the Ordinance, the Privacy Commissioner for Personal Data (the "PCPD") has substantial investigative powers, such as entering premises and requiring the production of documents, if they have reasonable grounds to believe an act has been committed in breach of the Ordinance. If a data user is found to be in breach of the Ordinance, the PCPD will generally issue an enforcement notice. Non-compliance of the notice is a criminal offence and is punishable by a maximum fine of HK$50,000 and a maximum term of imprisonment of 2 years.

III. IS GIVING OF DATA BREACH NOTIFICATION MANDATORY?

Readers may have heard of the General Data Protection Regulation ("GDPR"), which was adopted in the European Union in 2016 and came into force May this year. The GDPR involves certain provisions and rights that are not found under the PDPO. An obvious example is that, under the GDPR, data users generally must report breaches of personal data within 72 hours of notice of the breach, failing which the data users can be fined up to 2% of their annual global turnover.

Indeed, many jurisdictions other than the EU, such as Canada, Australia and many states in the United States, have similar rules making the disclosure and notification of data breaches mandatory with serious sanctions for non-compliance. However, notification of personal data breaches to either data subjects or the PCPD is not a mandatory requirement under the PDPO, though it was once proposed as part of the amendments in 2012, but ultimately did not form part of the current legislation. As such, generally speaking, there is no legal consequence for failing to give such a notification for a data breach in Hong Kong.

While not a legal requirement, the Commissioner does encourage notification of breaches. Data users must also consider the other potential backlash, such as a public relations crisis, as well as other sectoral laws and regulations that may be binding on data users and require data users to notify such breaches to relevant authorities, such as the Securities and Futures Ordinance (Cap. 571 of the Laws of Hong Kong) and the Listing Rules.

IV. TIPS ON PREVENTING DATA BREACHES

Needless to say, an up-to-date data security system would be useful in preventing data breaches as a result of hacking or computer intrusion. Aside from that, there are other simple measures that would significantly reduce the risk of data breaches.

A common pitfall is that data users does not keep track of the duration of possession of personal data. Although the PDPO does not stipulate a specific timeframe for when personal data has to be erased, it provides that "all practicable steps must be taken to ensure that personal data is not kept longer than is necessary for the fulfillment of the purpose." Data users often overlook the importance of clearing personal data collected. Indeed, the lesser the amount of data held by a data user, the smaller the impact of a data breach. In this connection, subsequent to the data breach incident of HKBN, HKBN has pledged to keep information for no more than 6 months. Such remedial move has received positive responses.

According to a recent research, over 40% of data breach incidents are attributable to the negligence or mistake of the employees. Data users must therefore carefully control and audit their internal policies and strictly adhere to the same in order to minimize the possibility of data breach caused by inadvertent employees. Recently, the UK Court has found an employer to be vicariously liable for the criminal actions of its employee in maliciously copying and making public the personal data of other employees despite the employer was found not be in breach of any data protection laws. As such, while regulatory compliance may only serve to protect a data user from primary liability, the data user can still be vicariously liable for the actions of their employees. Therefore, it is important for data users to be wary of the conduct of their employees by providing sufficient training, implementing access control and conducting regular internal audit.

V. HOW TO RESPOND TO A DATA BREACH CRISIS

To minimize the damage and liability, data users must react promptly and appropriately upon discovery of a data breach. In particular, the following immediate courses of action should be taken: -

(i) Identify the cause and source of the breach;

(ii) Adopt containment measures so as to halt further data breach; and

(iii) Assess the damage and loss.

Each of these steps is important to the minimization of impact of the breach as well as prevention of further breaches. Obtaining such information will also be crucial in any potential legal actions against the data user in proving that all practical steps have been taken to guard against potential data breaches. As such, it is strongly recommended to document the findings of the investigation.

Even the biggest multinational corporations may not be equipped for handling a significant data breach incident. Companies should therefore have a crisis management plan in place or at least know who to contact and bring in, such as legal advisors, investigators, cybersecurity experts and public relations advisers, when such situation is to occur. In particular, it is advisable to first contact legal advisors in the event of data breach so as to bring in the legal profession privilege, which prevent any information disclosed to the legal advisors from being used against the breaching party subsequently. More importantly, legal advisors can help analyze and assess the legal consequences and potential liability, coordinate the post-breach actions, and determine what information to share with external investigators and experts, whether there is a need to give notification of the data breach, to whom the notification is given, and the content of the notification.

VI. TAKEAWAYS

Following a series of data breach incidents, the public calls for the implementation of the mandatory data breach notification under the PDPO. It is expected that there will soon be reform in the PDPO and the data protection regime in Hong Kong. In the meantime, data users must review the data protection policies from time to time to ensure that there is no loophole that will lead to any inadvertent data breaches. It is advisable to seek early legal advice to ensure that the data protection policies comply with the current statutory requirements. In the midst of data breaches, it is also advisable to act promptly and contact legal advisors to coordinate the post-breach actions.