Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 15, NUMBER 1 >>> JANUARY 2015

Hong Kong Privacy Implications of Social Media, Mobile Computing, 'Big Data' and the Cloud: Contractual Protections to Negotiate with Providers

By Duncan Abate, Hong Tran and Anita Lam, of Mayer Brown JSM, Hong Kong.

Social media, mobile computing, "big data" analysis and cloud computing ("SMAC") are fundamentally changing the way in which companies can now operate.

In many ways, SMAC can help increase efficiency and improve outcomes in areas such as human resources ("HR"), particularly with HR processes such as talent acquisition, performance management and employee engagement.

However, using these technologies without understanding the legal risks and compliance issues could be dangerous and costly.

This article examines the use of SMAC from the perspective of Hong Kong data privacy law, and suggests terms that companies may wish to consider negotiating with their SMAC providers.

Data Privacy Obligations

Under the Personal Data (Privacy) Ordinance ("PDPO"), all HR related SMAC providers are likely to be regarded as "data processors", as they are engaged to process personal data of staff on behalf of the employers.

Employers, as data users, are expected to adopt "contractual or other means" to restrict:

- any personal data transferred to a data processor from being kept longer than is necessary (Data Protection Principle 2(3)); and
- unauthorised or accidental access, processing, erasure, loss or use of any personal data transferred to a data processor for processing (Data Protection Principle 4(2)).

These obligations apply regardless of whether the SMAC providers are based in Hong Kong. Under Section 65(2) of the PDPO, any data breach or misuse of the personal data by a data user's contractor (such as a SMAC provider) will be treated as carried out by the data user.

What Can Be Done?

From a data privacy perspective, a company should negotiate with its SMAC providers to ensure each service

contract contains terms to protect the employer's interests and comply with the PDPO.

The following sample clauses may help focus a company's discussion (as data user) with its SMAC providers. If it already has a SMAC contract, a company may consider writing to a SMAC service provider to set out the standard of security and confidentiality it expects from the service provider.

Warning: Please note that these sample clauses are intended for reference only and will need to be adapted to fit each company's situation. They are not "one-size-fits-all", and companies are advised to seek legal advice before adopting them.

Security Measures of the SMAC Provider

A SMAC provider should be expected to adopt a reasonable level of security measures to protect the personal data entrusted to it.

What practical measures should be adopted to safeguard the personal data entrusted to it will depend on many factors. These include:

- the nature or sensitivity of the personal data involved;
- whether such data is in hard copy or electronic form; and
- whether there are any relevant industry practices and standards, *etc.*

If the SMAC provider operates outside Hong Kong, the company may need to seek its assurance that its policies, procedures and processes are in compliance with local data privacy laws.

SAMPLE CLAUSE:

[SMAC Provider] must at all times employ reasonable organisational, operational and technological processes and procedures to keep the personal data safe from any unauthorised, accidental or unlawful use, access, alteration, loss, destruction, erasure, theft or disclosure.

The organisational, operational and technological processes and procedures adopted by [SMAC Provider] must at all times comply with:

a. the requirements under the Personal Data (Privacy) Ordinance;

b. the relevant guidelines and best practices recommended by the Office of the Privacy Commissioner for Personal Data from time to time; and

c. [any other relevant market practices or Data User's own internal policies].

[Data User] reserves the right to require [SMAC Provider] to improve the security or protection of the personal data if it is of the opinion that the processes and procedures taken by [SMAC Provider] are insufficient in any regard.

Restricting Access

Those SMAC employees who have access to the personal data should also be adequately trained in data protection procedures and policies. Their access to the data should be provided on a "need-to-know" basis.

SAMPLE CLAUSE:

[SMAC Provider] should ensure that:

a. only those employees required to carry out the services under this Agreement may have access to the personal data; and

b. such employees:

i. are provided with only the personal data they need to perform the services under the Agreement;

ii. are informed of the confidential nature of the personal data;

iii. have undergone adequate training with respect to data protection procedures and policies; and

iv. agree to comply with the obligations set out in this Agreement.

Restricting Use of Personal Data

It is important to limit the SMAC provider's use of the personal data to the purpose for which a company provides the personal data in the first place.

For example, if a company entrusts its SMAC provider with the personal data of its employees for HR analytics purposes, it is important that the company limit the SMAC provider's use of the personal data to that purpose, and not for its own purposes.

SAMPLE CLAUSE:

[SMAC Provider] must:

a. use the personal data only for the purpose(s) set out in this Agreement;

b. process the personal data in accordance with the instructions of [Data User]; and

c. process the personal data only to the extent, and in such manner, necessary for the proper provision of the services set out in this Agreement.

[SMAC Provider] must not perform this Agreement in such a way so as to cause [Data User] to breach any of its applicable obligations under the Personal Data (Privacy) Ordinance or any other applicable laws or regulations.

Transfer or Disclosure of Personal Data

The SMAC provider should not disclose or transfer any personal data of the employer to a third party, except with the express consent of the employer or where required by law.

SAMPLE CLAUSE:

[SMAC Provider] must not publish, disclose, divulge or transfer any personal data to any third party (whether within or outside Hong Kong) without the prior written consent of [Data User].

If [SMAC Provider] is required by law or legal process to disclose any personal data, it must promptly inform

   ISSN 1473-3579

[Data User] before any such disclosure, unless such notification is prohibited by law.

Subcontracting by the SMAC Provider

The Privacy Commissioner suggests that data users should restrict or ban SMAC providers from subcontracting their obligations under the service agreement to another third party.

The sample clauses below provide that subcontracting is permitted only with the express consent of the data user, and set out the responsibilities of the SMAC provider in engaging a subcontractor.

SAMPLE CLAUSE:

[SMAC Provider] must not subcontract any of its rights or obligations under this Agreement without the prior written consent of [Data User].

Where prior written consent is obtained from [Data User] in accordance with the clause above, [SMAC Provider] may subcontract its rights or obligations under this Agreement only by way of a written agreement with [Subcontractor] which imposes the same obligations on [Subcontractor] as are imposed on [SMAC Provider] under this Agreement.

Where [Subcontractor] fails to fulfil its obligations under any subcontracting agreement, [SMAC Provider] shall remain fully liable to [Data User] for the fulfilment of its obligations under this Agreement.

Deletion or Retention of Data

A SMAC provider should be expected to delete or return the personal data once the SMAC provider no longer needs them to carry out its obligations under the service agreement.

SAMPLE CLAUSE:

[SMAC Provider] must destroy all personal data promptly:

a. when they are no longer needed for [SMAC Provider] to perform the services for which [SMAC Provider] was retained; or

b. at the instruction of [Data User].

In complying with the clause above, [SMAC Provider] must ensure that:

a. all electronic copies of the personal data are removed from its systems by either destruction of the storage device (by drilling holes through the media or putting magnetic media through a degausser) or using appropriate electronic deletion software;

b. any printed copies are securely destroyed by cross-cut shredding and are not recycled; and

c. a record of such activities is maintained so to provide [Data User] with evidence of what records have been deleted/destroyed, when, by whom and by what method.

Notification of Data Security Breach

A SMAC provider must notify a data user where there has been a data security breach or data leakage. A company may also consider requiring the SMAC provider to take immediate steps to stop or rectify the security breach as soon as a breach is discovered.

SAMPLE CLAUSE:

Where there has been any unauthorised, accidental or unlawful use, access, alteration, loss, destruction, erasure, theft or disclosure of the personal data ("Security Breach"), [SMAC Provider] must report this to [Data User] as soon as [SMAC Provider] becomes aware of the incident of:

a. the personal data involved;

b. how the incident occurred;

c. those who were involved; and

d. the anticipated impact.

[SMAC Provider] must provide any assistance as required by [Data User] to rectify such Security Breach.

Indemnity from the SMAC Provider

The following suggested clause provides a company with a contractual remedy against its SMAC provider for any losses it suffers as a result of any non-compliance by the SMAC provider with the PDPO or the terms of the agreement.

SAMPLE CLAUSE:

[SMAC Provider] agrees to hold harmless and indemnify [Data User] against all claims, demands, actions, proceedings and expenses (including legal fees and disbursements) which arise or are connected with [SMAC Provider]'s provision of the services under this Agreement, including but without limitation to those arising out of any third party demand, claim or action, or any breach of contract, negligence, fraud, wilful misconduct, breach of statutory duty or non-compliance with any part of the Personal Data (Privacy) Ordinance by [SMAC Provider] or its employees, agents or subcontractors.

Further Tips

Additional Clauses

Apart from the above suggested clauses, a company may wish to consider:

- reserving the right to inspect the SMAC provider's systems; and
- requiring the assistance of the SMAC provider in complying with a data access request or data correction request made by a data subject.

What additional clauses are required or desirable will depend on various different factors, such as the type of work carried out by the SMAC provider, the nature or sensitivity of the personal data provided to the SMAC provider, relevant industry standards or market practice,

etc. For example, if the personal data provided to the SMAC provider are transported in hard copy format, then a company should consider the security measures required to safeguard the personal data during transport.

Other Tips

For cloud providers that have data centres in multiple countries, personal data entrusted to them may flow from one country to another based on an algorithm that optimises the use of the cloud provider's storage and processing resources.

For this reason, it is important to find out from the cloud provider:

- where the data will be stored; and
- whether it can be stored in countries that the company is reasonably certain have adequate legal and regulatory protections.

If a SMAC provider is based outside Hong Kong, a company should consider consulting a local expert to advise on the relevant data protection laws or regulations in that jurisdiction, and ensure that the agreement is enforceable against the SMAC provider in that jurisdiction.

Conclusion

Negotiating the terms of a SMAC agreement can be tricky, but a well-drafted agreement will not only discharge a company's liabilities under the Personal Data (Privacy) Ordinance, but also will help build trust and confidence with its SMAC provider as it removes any ambiguities and minimises future arguments.

Duncan Abate and Hong Tran are Partners and Anita Lam is a Consultant at Mayer Brown JSM, Hong Kong. They may be contacted at duncan.abate@mayerbrownjsm.com, hong.tran@mayerbrownjsm.com and anita.lam@mayerbrownjsm.com.

   ISSN 1473-3579