

## A Data User's New Obligations - Data Privacy Law That Has Teeth and Can Bite (Part 2)

### Summary

The Personal Data (Privacy) Amendment Ordinance 2012 will come into force in Hong Kong on 1st October 2012.

This email legal update is part of our series of updates to discuss its implications for employers and other data users.

In this email legal update, we look at a data user's obligations when engaging third party processors such as payroll agents, pension administrators, external IT consultants, and waste disposal/ shredding companies. We also look at ways of discharging these new obligations.

So, if you engage any of these third party data processors, it is time to reconsider your current arrangements with them to ensure you are in compliance with the Amendment Ordinance!

### Full Update

A number of significant changes will be brought about by the Personal Data (Privacy) Amendment Ordinance 2012 ("the Amendment Ordinance") when it comes into force on 1st October 2012.

In our legal update series, we will consider:

- (a) a data user's obligations in engaging third party data processors;
- (b) the changes to the Data Protection Principles and the new exemptions;
- (c) a delinquent employee's personal liability in misusing the personal data kept by his employer;
- (d) the Privacy Commissioner's new power to grant legal assistance to complainants; and
- (e) the Privacy Commissioner's greater power to issue Enforcement Notices and to impose heavier penalties.

In this email legal update, we focus on a data user's

obligations when engaging third party data processors.

### 1. The Current Position:

Under section 65 of the Personal Data (Privacy) Ordinance (PDPO), a data user is generally liable for the acts and practices of the agents it engages.

Data Protection Principle (DPP) 2 of the PDPO provides that personal data must not be kept longer than is necessary to fulfil the purpose for which the data are used.

DPP4 further provides that all reasonably practicable steps must be taken to ensure that personal data held are protected against unauthorised access, processing, erasure or other use.

If a data user's agent is found to have contravened these DPPs, then the wrongful act is treated as an act done by the data user as well as its agent. There is no apparent "escape hatch" for a data user to exonerate itself from the wrongful acts of its agent.

### 2. What is new?

#### 2.1 DEFINITION OF "DATA PROCESSOR"

Under the Amendment Ordinance, the term "data processor" is introduced and is defined in the DPP set out in Schedule 1 as being a person who:

*"(a) processes personal data on behalf of another person; and*

*(b) does not process the data for any of the person's own purpose."*

This is a very wide definition which includes various third party agents commonly used by companies such as payroll agents, pensions administrators, external IT consultants/ companies, survey companies and even companies engaged to dispose of/ shred documents.

## 2.2 NEW OBLIGATIONS UNDER DPP2 AND DPP4

Under the Amendment Ordinance, the new DPP2 and DPP4 now impose express requirements on a data user to ensure its agents are in compliance with these DPPs.

Under the new DPP2 and DPP4, data users must adopt “*contractual or other means*” to prevent:

- (a) any personal data transferred by the data user to a data processor from being kept longer than is necessary for processing of data (in the case of DPP2); and
- (b) unauthorised or accidental access, processing, erasure, loss or use of any personal data transferred by the data user to a data processor for processing (in the case of DPP4).

It is important to note that these obligations are mandatory and they apply regardless of whether the data processor is based within or outside Hong Kong.

## 3. The Views of the Privacy Commissioner

### 3.1 CONTRACTUAL MEANS TO ENSURE COMPLIANCE WITH DPP2 AND DPP4

To help a data user discharge these new obligations, the Privacy Commissioner has suggested a number of provisions which a data user may include in its contract with a data processor. These include:

- a requirement for the data processor to adopt security measures to protect the data in question;
- a procedure for the data processor to return or destroy the data;
- a restriction on the use of such personal data by the data processor;
- a restriction or ban on the data processor from outsourcing or sub-contracting its data processing functions;
- a requirement for the data processor to immediately inform the data user in the event of any data leakage;
- a requirement for the data processor to adopt adequate data protection policies/ procedures and to provide adequate training to its staff to ensure compliance with such policies/ procedures.

Apart from the contractual provisions suggested above, a data user may also consider including an indemnity clause in its agreement with the data processor, so that it has a contractual remedy against the data processor for any losses it suffers as a result

of any non-compliance by the data processor with the Amendment Ordinance.

### 3.2 OTHER MEANS TO ENSURE COMPLIANCE WITH DPP2 AND DPP4

The Privacy Commissioner has also suggested a number of “other means” for data users to consider to ensure compliance with the Amendment Ordinance. These include:

- selecting a reputable data processor with adequate means to protect the personal data in question;
- ensuring the data processor has adequate data protection policies/ procedures and that its staff are trained in this area; and
- inspecting the ways in which the data processor stores the personal data and the security measures implemented (e.g., through site visits).

There are also a number “best practices” which a data user should consider adopting. These include:

- adopting clear and transparent policies and procedures on data protection and security;
- ensuring any contractual arrangement with overseas data processors are enforceable in Hong Kong;
- documenting clearly the type of personal data provided or transferred to data processors; and
- considering whether to redact personal data (or any information which may identify an individual) before providing or transferring such data to data processors.

## 4. What does this mean?

### 4.1 CONSEQUENCES OF NON-COMPLIANCE

A failure to comply with the new requirements with respect to data processors constitutes a breach of the DPPs.

Moreover, if any individual suffers any loss or damage caused by the wrongful act of the data user’s agent, he or she may bring legal proceedings against the data user (and its agent) to seek compensation.

### 4.2 TIPS FROM US

We recommend that in adopting the means suggested above (particularly those set out in 3.2 above), a data user should keep a record of the steps it has taken to ensure compliance with DPP2 and DPP4.

In particular, it should be noted that the new DPP2 and DPP4 requires “*all reasonably practicable steps*” to be taken by a data user to comply with these requirements. A data user should have a reasonable defence under DPP2 and DPP4 if it can demonstrate to the Privacy Commissioner that it has taken all reasonably practicable steps to ensure it complies with such requirements by carefully selecting reputable data processors as its service providers and by including the necessary safeguards in its contracts with them.

## 5. Conclusion

To minimize the risk of non-compliance with the new requirements under the Amendment Ordinance, data users would be well advised to review and, where appropriate, strengthen their own policies and procedures for appointing data processors and overseeing their performance on an ongoing basis.

If you wish to learn more about the other changes to the PDPO, stayed tuned!

## Contact Us

For inquiries related to this Legal Update, please contact the following person or your usual contacts with our firm.

### **Duncan Abate**

Partner

T: +852 2843 2203

E: [duncan.abate@mayerbrownjism.com](mailto:duncan.abate@mayerbrownjism.com)

### **Hong Tran**

Partner

T: +852 2843 4233

E: [hong.tran@mayerbrownjism.com](mailto:hong.tran@mayerbrownjism.com)

### **Anita Lam**

Consultant

T: +852 2843 4536

E: [anita.lam@mayerbrownjism.com](mailto:anita.lam@mayerbrownjism.com)

### **Stephanie Chiu**

Associate

T: +852 2843 2293

E: [stephanie.chiu@mayerbrownjism.com](mailto:stephanie.chiu@mayerbrownjism.com)

---

Mayer Brown JSM is part of Mayer Brown, a global legal services organisation advising clients across the Americas, Asia and Europe. Our presence in the world's leading markets enables us to offer clients access to local market knowledge combined with global reach.

We are noted for our commitment to client service and our ability to assist clients with their most complex and demanding legal and business challenges worldwide. We serve many of the world's largest companies, including a significant proportion of the Fortune 100, FTSE 100, DAX and Hang Seng Index companies and more than half of the world's largest banks. We provide legal services in areas such as banking and finance; corporate and securities; litigation and dispute resolution; antitrust and competition; employment and benefits; environmental; financial services regulatory & enforcement; government and global trade; intellectual property; real estate; tax; restructuring, bankruptcy and insolvency; and wealth management.

OFFICE LOCATIONS AMERICAS: Charlotte, Chicago, Houston, Los Angeles, New York, Palo Alto, Washington DC  
ASIA: Bangkok, Beijing, Guangzhou, Hanoi, Ho Chi Minh City, Hong Kong, Shanghai, Singapore  
EUROPE: Brussels, Düsseldorf, Frankfurt, London, Paris  
TAUIL& CHEQUER ADVOGADOS in association with Mayer Brown LLP: São Paulo, Rio de Janeiro  
ALLIANCE LAW FIRM: Spain (Ramón y Cajal Abogados)

Please visit [www.mayerbrownjism.com](http://www.mayerbrownjism.com) for comprehensive contact information for all Mayer Brown offices.

This publication provides information and comments on legal issues and developments of interest to our clients and friends. The foregoing is intended to provide a general guide to the subject matter and is not intended to provide legal advice or be a substitute for specific advice concerning individual situations. Readers should seek legal advice before taking any action with respect to the matters discussed herein. Please also read the Mayer Brown JSM legal publications Disclaimer.

Mayer Brown is a global legal services provider comprising legal practices that are separate entities (the “Mayer Brown Practices”). The Mayer Brown Practices are: Mayer Brown LLP and Mayer Brown Europe – Brussels LLP, both limited liability partnerships established in Illinois USA; Mayer Brown International LLP, a limited liability partnership incorporated in England and Wales (authorized and regulated by the Solicitors Regulation Authority and registered in England and Wales number OC 303359); Mayer Brown, a SELAS established in France; Mayer Brown JSM, a Hong Kong partnership and its associated entities in Asia; and Tauil & Chequer Advogados, a Brazilian law partnership with which Mayer Brown is associated. “Mayer Brown” and the Mayer Brown logo are the trademarks of the Mayer Brown Practices in their respective jurisdictions.

© 2012. The Mayer Brown Practices. All rights reserved.