Crossing Borders: New Guidance on the Transfer of Personal Data Outside Hong Kong

Gabriela Kennedy
Mayer Brown JSM, Hong Kong

Karen H.F. Lee*
Mayer Brown JSM, Hong Kong

Data controllers; Due diligence; Hong Kong; Personal data; Transborder data flows

Section 33 of the Hong Kong Personal Data (Privacy) Ordinance (PDPO), which restricts the cross-border transfer of personal data, has been in the statutory books since the PDPO was enacted in 1996. It has not yet been brought into force.

The Privacy Commissioner (PC) indicated a few years ago that s.33 would be enacted in the future and, to this end, his office commissioned research on the treatment of cross-border transfers in other jurisdictions. On December 29, 2014 the PC issued a new guidance on the transfer of personal data out of Hong Kong, to help data users prepare for the implementation of s.33 (Guidance Note).[1]

Section 33 of the PDPO

Once s.33 is in force, it will only be possible to transfer personal data outside Hong Kong if one of the following exceptions applies:

- the country to which the personal data will be transferred is part of a "white list" of jurisdictions which the Privacy Commissioner considers to have laws that protect personal data to a level commensurate with the PDPO;
- the data user has reasonable grounds to believe that the place to which the data is to be transferred has in force any law which is substantially similar to, or serves the same purposes as the PDPO;
- the data subject has consented in writing to the transfer;
- the data user has reasonable grounds to believe that the transfer is for the avoidance or mitigation of any adverse action against the data subject, and it is not practicable to obtain the data subject's consent, but if it were, then such consent would be given;
- the personal data is exempt from data protection principle (DPP) 3 of the PDPO by virtue of an exemption under the PDPO; or
- the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not be collected, held, processed or used in a manner that would constitute a contravention of the PDPO.

The PC's prior consent is not required in order for a data user to transfer personal data out of Hong Kong. However, if a data user's cross-border transfer is challenged by a data subject or the PC, then it will be up to the data user to prove that at least one of the above exceptions applies. A transfer of personal data in breach of s.33, once it comes into force, may result in the imposition of a fine of up to HK$10,000 and the issuance of an enforcement notice by the PC, requiring steps to be taken to rectify or prevent the recurrence of the breach. Breach of an enforcement notice will amount to a further offence, and can attract a fine of up to HK$50,000 and two years' imprisonment for a first conviction.

What transfers will be covered by s.33?

Section 33 will cover not only the transfer of personal data from Hong Kong to a country outside Hong Kong, but also any further transfers that occur between two different countries if the transfer is controlled by a data user in Hong Kong.

Examples of when s.33 will apply include:

- the transmission of personal data to offshore third-party service providers who provide outsourced services;
- the storing of personal data in the cloud, if the cloud server is located overseas or can be accessed by anyone outside of Hong Kong;
- the sharing of personal data with affiliated companies around the world; and
- the remote access and downloading by employees outside Hong Kong of personal data stored on servers located in Hong Kong.

Of the examples above, the last is probably the most difficult to accept given the mobility of the modern workforce and the fact that access to data at home when travelling overseas is normally made on devices that couple access with downloading. A refinement of this

* Gabriela Kennedy is a Partner and Karen H.F. Lee an Associate at Mayer Brown JSM, Hong Kong.
[1] See *http://www.pcpd.org.hk/english/resources_centre/publications/guidance/fact1_intro_1.html* [Accessed March 23, 2015].

example may be needed by including volume or intention triggers. Further guidance from the PC on this will no doubt be available once s.33 comes into force.

Personal data merely being transferred between two recipients in Hong Kong, but where owing to internet routing the personal data is being transmitted via a place outside Hong Kong, will not fall within the scope of s.33, provided no personal data are actually accessed or stored outside Hong Kong.

Who will be subject to s.33?

The PDPO distinguishes between a "data user" and a "data processor". A data user is a legal entity which either alone or jointly, or in common with another, controls the collection, holding, processing or use of personal data. By contrast, a data processor is a legal entity which merely holds, processes or uses personal data solely on behalf of another (i.e. the data user), and not for its own purposes.

Data processors are not directly regulated under the PDPO, as data users are ultimately responsible for compliance with the PDPO, and remain liable for any breach of the PDPO caused by their data processors. Data users must therefore ensure that any cross-border transfer to or by the data processor is in compliance with s.33. This is nothing new or revolutionary. The pitfalls of the data user/data processor agency relationship described above have been highlighted in the last couple of years through notorious cases that have made the headlines. Guidance notes issued by the PC on the amendments to the PDPO have also highlighted the fact that data users must ensure, by contractual or other means, that their data processors are required to comply with the rest of the PDPO (including the DPPs) in their use, processing and storage of the personal data, to reduce the data users' risk of being in breach of the PDPO owing to the actions of its data processors.

What guidance is provided by the Guidance Note?

The new Guidance Note supersedes the previous guidance issued by the PC on cross-border transfers in April 1997, which included a recommended model contract based on a precedent prepared by the Council of Europe, the Commission of the European Communities and the International Chamber of Commerce in the 1990s[2] (Former Guidance). The new Guidance Note retains some of the points made in the Former Guidance, but expands on each exception under s.33 and provides recommended model clauses, some mandatory (core), others optional (additional). Unlike in the model contract contained in the Former Guidance, the Guidance Note recommends Hong Kong governing law, and resolution of disputes stemming from the transfer agreement taking place in Hong Kong. The Former Guidance allowed foreign governing law and envisaged the settlement of disputes through arbitration in Hong Kong.

We have summarised below the comments and advice provided under the Guidance Note in relation to each of the above exceptions.

"White list" exemption

In 2013, the PC carried out a survey of 50 jurisdictions, and provided the Government with a proposed list of countries to be included in the white list for s.33.[3] However, the survey has not yet been made public and no final version of the white list has been gazetted. When finalised, the white list is intended to be a "live" document that is constantly re-evaluated and updated to take into account the changing laws of different jurisdictions.

In reality, it may take the PC and the Government a long time to finalise the white list and/or to add or remove any jurisdictions in the future. The time and effort it takes for an assessment of a jurisdiction to be completed is clearly demonstrated by the comparable cross-border data privacy laws of the EU. Under the EU Data Protection Directive, personal data may be transferred out of the European Economic Area, without needing to satisfy the other exceptions under the Directive, if the transfer is to a country that the European Commission believes provides adequate protection (the equivalent of Hong Kong's white list). So far, only 12 countries have been recognised by the European Commission as providing adequate protection, and have been included in the EU's white list. New Zealand was only added to the EU's white list in December 2012. Australia is a notable absence and other Asian countries have yet to be added.

In light of the above, data users should not simply assume that the jurisdictions to which they may transfer personal data in the future will be included in the PC's white list. Instead, we would recommend that data users build into their current practice a requirement that: (1) the data subject's prescribed consent to any transfer be obtained at the time their personal data are collected; (2) they have in place a data transfer agreement with the recipient of the data, consistent with the PDPO; and/or (3) that an audit be conducted regarding each potential recipient of the personal data before the transfer occurs. These are discussed further below.

Laws substantially similar to, or which serve the same purposes as the PDPO

To rely on this exception, the data user must have reasonable grounds, based on a professional assessment and evaluation, to believe that a country has in place laws that are substantially similar to, or serve the same purposes as the PDPO. Subjective belief would be insufficient, and a detailed assessment of the data privacy

[2] "Fact Sheet — Transfer of Personal Data Outside Hong Kong: Some Common Questions" (April 1997), *http://www.pcpd.org.hk/english/resources_centre/publications/guidance/fact1_intro_1.html* [Accessed February 23, 2015].
[3] See *http://www.legco.gov.hk/yr13-14/english/panels/ca/papers/cacb2-790-1-e.pdf* [Accessed February 23, 2015].

laws would need to be carried out. Relying on this exception could therefore be quite costly, as professional advice would need to be obtained. It is also not clear who will be qualified or willing to provide data users with such advice. Overseas and local lawyers may not be comfortable with signing off a statement confirming that the local laws of the country to which the personal data will be transferred are equivalent to the PDPO.

This exception is also intended to apply only in relation to countries which have not yet been assessed by the PC for the purposes of the white list. If the PC has already assessed the laws of a jurisdiction, but has rejected them as being inadequate and has therefore not included such country in the white list, then it is highly unlikely that a data user can rely on this exception in respect of that particular jurisdiction.

Considering the costs, difficulties and risks associated with relying on this exception, we believe that this should be one of the last resorts if the other exceptions to s.33 cannot be relied upon.

Consent in writing

Data users can carry out cross-border transfers of personal data if the data subject's prior consent is obtained in writing, and such consent is not subsequently withdrawn. On or before obtaining the data subject's consent, the data user must inform them of: (1) the purpose of the transfer; (2) the classes of persons to whom the personal data will be transferred; and (3) any consequences of providing their consent, e.g. a lower level of protection provided by the country to which his personal data will be transferred. Such information must be provided in a clear and easily understandable manner, along with a separate tick box so that the data subject can separately indicate their consent. It is recommended that such information be incorporated in the personal information collection statement provided to data subjects at the time their personal data is collected, and the data subject be required to tick a box and sign the personal information collection statement (or the form to which it is attached) to indicate their consent. If their personal data is collected online, then a requirement for them to click a box or an "I accept" button relating to the transfer should be incorporated.

Necessary to avoid or mitigate any adverse action

In order to rely on this exception, the data user must be able to establish that the transfer is necessary to protect the data subject's interests, and it is not feasible for their prior consent to be obtained. An example is if the transfer is required in order to perform a contract that the data subject is a party to, and failing to transfer the data would cause the data subject to suffer substantial financial loss. The PC anticipates that this exception will only apply in very limited circumstances.

We would recommend that this exception only be relied upon in extremely clear-cut cases that very obviously fall within its scope.

Exemptions to DPP 3

DPP3 prohibits data users from using personal data for a new purpose that is different from the original purpose of collection (or a directly related purpose), unless voluntary and explicit consent to the new purpose is obtained from the data subject. Part VII of the PDPO sets out a number of exemptions to the restriction under DPP3. These same exemptions can also be relied on by a data user for the transfer of personal data out of Hong Kong. These include the following:

- where the transfer is required for preventing or detecting a crime;
- where the transfer is required to prevent, preclude or remedy any unlawful or seriously improper conduct, dishonesty or malpractice;
- where the identity, location and health-related personal data of an individual must be disclosed to prevent serious harm to an individual's physical or mental health; and
- where the transfer is to a data user who is in the business of reporting the news, and there are reasonable grounds for believing that publication or broadcasting of the personal data are in the public interest.

Reasonable precautions and exercise of due diligence—data transfer agreements and due diligence

Having in place an enforceable contract between the data user and the recipient of the personal data is one of the best ways of demonstrating that all reasonable precautions have been taken in order to satisfy this exception. Even if s.33 is not yet in force or another exception under s.33 can be relied on, having such a contract is generally recommended as a matter of good practice.

Any contract between the data user and a recipient of the personal data should include provisions that require the person receiving the personal data to comply with the PDPO, particularly DPP2 (accuracy and retention of personal data), DPP3 (use of personal data), DPP 4 (security of personal data), DPP 5 (public availability of policies) and DPP6 (right to data access and correction). This will reduce both the risk exposure of the data user and the chances of the personal data being mishandled by the recipient. The Guidance Note sets out new model clauses that can be included in data transfer agreements between data users and recipients, to ensure compliance with the PDPO. These are discussed further below.

As an alternative to entering into a data transfer agreement with the recipient, a data user may instead audit and inspect the recipient's policies and practice to

ensure that they are in compliance with the PDPO. As part of the due diligence and audit, the data user should ensure that:

- the recipient has in place sufficient organisational and technical measures and policies, including adequate training for staff and effective security measures, to properly safeguard the personal data and to prevent them from being kept longer than necessary or from being used for any purposes that are not permitted;
- the recipient has not been involved in any data breaches in the past;
- the data subjects' rights of access and correction under the PDPO will not be affected by the transfer; and
- the data user has the right to audit and inspect (and conducts such audits and inspections regularly on) how the recipient uses and processes personal data to determine whether they comply with the PDPO.

If the overseas transfer is to an affiliated entity, the data user must still be satisfied that the relevant affiliate, and the group as a whole, have sufficient internal safeguards and policies in place that are consistent with the PDPO.

The carrying out of the above due diligence and audit may be most appropriate where the recipient will be processing, using or storing personal data on behalf of the data user on a long-term basis, e.g. where the data user has outsourced its payroll management services to an overseas company. In such circumstances, where the long-term processing and nature of the personal data mean that the risks of a breach or mishandling are high, and the consequences could be severe, it is advisable for the data user to conduct due diligence and audits of the recipient—even if a data transfer agreement is entered into with the recipient. Changes to the services being provided by the recipient, or even to the law or guidance provided by the PDPO, may lead to a data transfer agreement eventually becoming outdated. It is therefore important that data users also conduct due diligence and audits, both prior to the transfer of personal data and on an ongoing regular basis, to ensure compliance.

Where the transfer of personal data is a one-off event, or is provided under a short-term or limited contract (e.g. where a recruitment agency collects and processes personal data of job applicants on behalf of a data user), then it may not be cost-effective for the data user to conduct a due diligence exercise or audit. Instead, entering into a contract with the recipient that is consistent with the model clauses may be more appropriate.

Model clauses

The new model clauses expand the restrictions and obligations of the recipient in respect of personal data, which reflect the data users' obligations under the DPPs. For example, the requirement to obtain a data subject's prescribed consent in relation to any new purpose has always been an obligation under DPP3 of the PDPO. However, while this was implied in the 1997 model contract (i.e. recipients had to undertake to only use the personal data for the purposes listed in the cross-border agreement), the new revised model clauses make this explicit as the transferee is required to obtain the prescribed consent of the data subject for any new purpose of use.

While the core clauses are mandatory, the exact wording in the Guidance Note is not. This means that the clauses can be modified as required to meet the circumstances of a particular cross-border transfer. It is the "essence" of the core model clauses that needs to be incorporated in any data transfer agreement, rather than their exact wording.

The Guidance Note also proposes additional clauses, other than the core model clauses, which parties may consider including in their data transfer agreements. These additional clauses include the conferring of rights on data subjects, by virtue of the Contracts (Rights of Third Parties) Ordinance.[4] Pursuant to the new Contracts (Rights of Third Parties) Ordinance, data transfer agreements can be expressed for the benefit of the data subjects, who will therefore have a right to bring a legal action directly against the recipient of their personal data if the recipient breaches the data transfer agreement between it and the data user, notwithstanding the fact that the data subject was not a party to that agreement.

Once the Contracts (Rights of Third Parties) Ordinance comes into effect, the exclusion or inclusion of the data subjects' right to enforce the provisions of the outsourcing/data transfer agreement against the data processor will become a bargaining chip in contractual negotiations between data users and data processors. Data users may want such a provision, but they should note the requirement to provide data subjects with a copy of the agreement with the data processors.

The Guidance Note already contains a core clause that stipulates the apportionment of liability, vis-à-vis data subjects, between data users and data processors (cl.3.1). This may indeed be the preferred option in a data transfer agreement, though presumably the apportionment of liability would be triggered only in situations where there is fault on both sides, while an indemnity clause in favour of the data user would be needed for situations where the fault lies entirely with the data processor.

[4] Enacted on December 5, 2014. It will come into operation on a date to be prescribed by the Hong Kong Government.

What are the current legal requirements in force in relation to the transfer of personal data?

Even though s.33 has not yet come into operation, existing statutory requirements under the PDPO already impose requirements on data users that may affect their cross-border transfer of personal data. In brief, these other requirements under the PDPO are as follows:

General notification requirements (DPP 1(3))

On or before the collection of an individual's personal data, data users must ensure that the relevant data subject is informed (amongst other things) of the classes of persons to whom the data may be transferred to and the purpose of such transfer. As such, if the data user will be transferring any personal data to a third party service provider or affiliate located either inside or outside Hong Kong, then this should be notified to the data subject at the time that his/her personal data is collected.

Prescribed consent for any new purpose (DPP 3)

If the data user intends to transfer any personal data to a third party service provider or affiliate (whether or not they are located inside or outside of Hong Kong), and such transfer was not within the original purpose (or a directly related purpose) of collection, then the data subject's express and voluntary consent must be obtained beforehand.

Direct marketing requirements (Pt VIA)

If a data user intends to transfer personal data to a third party for the purposes of direct marketing (e.g. the third party will make direct marketing calls on behalf of the data user), then the date user must obtain the relevant data subject's prior written consent. The data user must explicitly notify the data subject in writing beforehand of its intention to transfer the personal data to a third party for direct marketing purposes and whether the transfer is made in return for gain, e.g. money or other property. The data subject must have explicitly indicated in writing that he/she does not object to the use and transfer for the purposes of direct marketing.

Data processors (DPP2 (3) and DPP 4(2))

If a data user engages a data processor (including any other entity within the same group), to use, store or process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than is necessary, and to prevent any unauthorised or accidental access, processing, erasure, loss or use of the personal data by the data processor.

Note that even after s.33 comes into operation, data users will still be obligated to also comply with the above requirements under the PDPO.

Breach of these obligations may result in an enforcement notice being issued by the PC against the data user requiring it to take certain steps or measures to rectify or prevent any recurrence of the breach. Failing to comply with an enforcement notice constitutes an offence, which attracts a maximum fine of HK$50,000 and two years' imprisonment, and a daily penalty of HK$1,000 for any continuing offence. Further penalties will also apply for any subsequent repeat contraventions on the same facts or for multiple breaches of enforcement notices.

Breach of the direct marketing requirements constitutes an offence, and incurs a higher maximum fine of HK$500,000 and three years' imprisonment. Where the breach involves the sale or transfer for gain of any personal data to a third party for direct marketing purposes, then the maximum fine is HK$1,000,000 and five years' imprisonment.

Conclusion and recommendations

No official announcement has been made by the PC as to when s.33 will come into force. However, in anticipation of s.33 eventually coming into force in the future, data users are advised to review their current cross-border transfer practices to ensure consistency with the Guidance Note and s.33.

We would recommend that the best way for a data user to ensure compliance with s.33 is to:

- obtain each data subject's consent to the transfer of their personal data overseas pursuant to the exception under s.33 (discussed above), and such consent should be obtained at the time that the data subject's personal data are collected. The required information can be incorporated in the relevant personal information collection statement provided to data subjects at the time of collection of their personal data, and should also include a tick box enabling the data subject to indicate their specific consent to the cross-border transfer. Note that this will need to be in addition to and separate from any consent (and therefore any tick box) relating to the transfer of personal data for direct marketing purposes;
- enter into data transfer agreements with the intended recipients of the personal data that incorporate the PC's recommended model clauses (amended as necessary to suit the relevant circumstances); and/or
- conduct an audit on the intended recipients of the personal data to ensure that they have in place policies and practices that are consistent with the PDPO.

Even though s.33 is not yet in operation, existing obligations under the PDPO apply to all transfers of personal data. Data users should therefore review their internal policies and practices, as well as their existing and future contracts with data processors, in order to ensure compliance with both the existing requirements under the PDPO and s.33. Taking a proactive approach is the best way for data users to mitigate any potential liability.