Guidance on Personal Data Protection in Cross-border Data Transfer

PART 1: INTRODUCTION

Section 33 of the Personal Data (Privacy) Ordinance (the "**Ordinance**") prohibits the transfer of personal data to places outside Hong Kong unless one of a number of conditions is met. The purpose of such cross-border transfer restriction is to ensure that the transferred personal data will be afforded a level of protection comparable to that under the Ordinance.

Although section 33 is not yet effective, this Guidance serves as a practical guide for data users to prepare for the implementation of section 33 of the Ordinance. It helps data users to understand their compliance obligations for cross-border data transfer once section 33 is effective. All the conditions for waiving the transfer restriction are dealt with in this Guidance.

Regardless of when section 33 will take effect, data users are encouraged to adopt the practices recommended in this Guidance as part of their corporate governance responsibility to protect personal data.

The legal requirements

Section 33(2) specifies that a data user shall not transfer personal data to a place outside Hong Kong unless one of the following conditions is met:

(a) The place is specified by the Privacy Commissioner for Personal Data (the "**Commissioner**") by notice in the Gazette that there is in force any law which is substantially similar to, or serves the same purposes as, the Ordinance;

(b) The data user has reasonable grounds for believing that there is in force in that place any law which is substantially similar to, or serves the same purposes as, the Ordinance;

(c) The data subject has consented in writing to the transfer;

(d) The data user has reasonable grounds for believing that the transfer is for the avoidance or mitigation of adverse action against the data subject; it is not practicable to obtain the consent in writing of the data subject to that transfer; but if it was practicable, such consent would be given;

(e) The data is exempt from Data Protection Principle ("**DPP**") 3 by virtue of an exemption under Part VIII of the Ordinance; or

(f) The data user has taken all reasonable precautions and exercised all due diligence to ensure that the data will not, in that place, be collected, held, processed, or used in any manner which, if that place were Hong Kong, would be a contravention of a requirement under the Ordinance.

Section 33 and DPPs

DPP3, which is directed against the misuse of personal data, specifies that personal data shall not, without the data subject's prescribed consent, be used for a new purpose. "New purpose" means in essence any purpose other than the one for which the personal data was originally collected or a directly related purpose. "Prescribed consent" means consent that is expressly and voluntarily given and has not been withdrawn by the data subject in writing, while "use" includes both disclosure and transfer of data. Thus, transfer of personal data to a place outside Hong Kong would require the data subject's prescribed consent under DPP3 if it is for a new purpose unless such transfer falls within the exemptions under Part VIII of the Ordinance.

Further, the trend of outsourcing and entrusting personal data processing work by data users to their agents is increasingly common. If a data user engages a data processor to process personal data outside Hong Kong on the data user's behalf, the data user must adopt contractual or other means to (i) prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data (under DPP2(3)), and (ii) prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing (under DPP4(2)). If a data user passes customers' personal data to a contractor situated outside Hong Kong to make direct marketing phone calls, it is still required to observe the requirements under Part VIA of the Ordinance in using personal data in direct marketing. The data user remains liable for the act done by its agent with its authority under section 65 of the Ordinance.

Data users are therefore reminded that compliance with section 33 does not exonerate their obligation under other requirements of the Ordinance.

Contravention

Data users who, without reasonable excuse, contravene section 33 commit an offence under section 64A of the Ordinance, which carries a fine of up to HK$10,000. The Commissioner may also issue enforcement notices to data users who have contravened section 33 or DPP[1]. Contravention of an enforcement notice issued by the Commissioner is an offence which carries a fine and imprisonment, and a daily penalty in the case of a continuing offence after conviction[2].

Who is required to comply with section 33?

Section 33 applies to a "data user", which is defined under section 2(1) of the Ordinance to mean, in relation to personal data, a person who either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data.

Pursuant to section 2(12) of the Ordinance, a person who is merely transmitting data on behalf of another and not for any of his own purposes is not a data user in relation to that data. It follows that such person, not being a data user, is not required to observe section 33. For example, when a telecommunication service provider transmits personal data for other data users, it is not required to observe section 33 in relation to the data it transmitted. On the other hand, a person using telecommunication means to transfer the data under his control will be subject to section 33.

What types of transfers are subject to section 33?

Section 33 covers two situations, namely (i) transfers of personal data from Hong Kong to a place outside Hong Kong, and (ii) transfers of personal data between two other jurisdictions where the transfer is controlled by a Hong Kong data user.

---

[1] Section 50.
[2] Section 50A.

The Ordinance itself does not define 'transfer'. The ordinary meaning of the word, which is transmission from one place or person to another, applies. Transfer is distinguished from mere transit.

Transferring data outside Hong Kong is often associated with the act of sending or transmitting personal data from Hong Kong to another jurisdiction for storage and/or processing, for instance, by sending paper or electronic documents containing personal data by courier, post or electronic means. Transfer of data becomes a complex issue with the use of the Internet and emerging technology. Data movements across the borders can take various forms, and it may not be straightforward to determine whether certain movement of personal data constitutes a 'transfer' for the purpose of section 33. It depends on the circumstances.

It must be borne in mind that the act of storing personal data outside Hong Kong will trigger the application of section 33.

Examples of whether transfer of personal data outside Hong Kong under section 33 has taken place:

✓ Engaging a third party service provider situated outside Hong Kong to process personal data on its behalf regardless of the physical location of personal data storage

✓ Passing customers' personal data to contractor situated outside Hong Kong to make direct marketing phone calls

✓ Sharing personal data of customers and/or employees with sister companies in the same holding company around the world by storing the data in a centralised database

✗ Sending an email to a Hong Kong recipient during which process the data is transmitted via a server/equipment situated outside Hong Kong because of Internet routing

✗ Unauthorised access of personal data by third parties outside Hong Kong, such as hacking[3]

In the above examples of engaging third party service providers, the data users "consciously" engage outside parties to handle personal data and the process involves data transfer outside Hong Kong. Data users who are in possession of personal data owe a duty to data subjects to ensure that the third party service provider will not engage in any act such as storage and/or processing of personal data outside Hong Kong without complying with section 33.

For the avoidance of doubt, the transfer of personal data by one person located in Hong Kong, but because of Internet routing through a place outside Hong Kong (without being accessed or stored as part of the transmission mechanism), to a recipient also located within Hong Kong does not fall under the scope of section 33. However, the position will be different where the targeted recipient is located outside Hong Kong. In addition, if a multi-national corporation stores personal data in an internal server located in Hong Kong but its employees working in offices outside Hong Kong are allowed to download the personal data, it is considered as an arrangement falling under the scope of section 33.

Storing personal data in the cloud may also constitute a transfer outside Hong Kong if the cloud server is accessible outside Hong Kong. Data users should be mindful of their obligations under section 33 of the Ordinance in engaging cloud service provider and using cloud to store and/or process personal data.

[3] In those circumstances, there may be an issue whether DPP4 that governs data security has been duly observed by data users. Data users should refer to the "Guidance on Data Breach Handling and the Giving of Breach Notifications" issued by the Commissioner.

PART 2: EXCEPTIONS TO CROSS-BORDER TRANSFER RESTRICTIONS UNDER SECTION 33(2)

A data user is required to comply with any one of the exceptions as specified under section 33(2) of the Ordinance in order to remove the cross-border transfer restrictions. For the avoidance of doubt, fulfilment of any one of the exceptions will suffice for complying with section 33. Nevertheless, it is a good practice for a data user to adopt multiple measures (if practicable) to enhance the protection afforded to the personal data transferred across the border. For example, even if the recipient of the personal data is located in a place specified by the Commissioner as having in force in that place any law which is substantially similar to, or serves the same purposes as, the Ordinance (exception under section 33(2)(a)), a data user may still, as a good practice, enter into contract with the recipient to provide for specific contractual requirements on protection of personal data (exception under section 33(2)(f)).

Section 33(2)(a) White List jurisdictions as specified by the Commissioner in the Gazette

The Commissioner will assess and evaluate the data protection regimes of other jurisdictions to determine whether there is in force "*any law which is substantially similar to, or serves the same purposes as*" the Ordinance. This essentially requires a determination by the Commissioner on whether personal data is protected in that jurisdiction to a level which is commensurate with the Ordinance, so that the protection afforded to any personal data transferred outside Hong Kong will be substantially in the same scope and depth as that provided under the Ordinance.

A list of jurisdictions, which the Commissioner determines to have in force "*any law which is substantially similar to, or serves the same purposes as*" the Ordinance, will be specified by notice in the Gazette by the Commissioner (the "**White List**") under section 33(3). The White List is a living document subject to the Commissioner's review. The Commissioner may add or subtract[4] the jurisdictions on the list in light of their changing legislative positions on data protection.

It is permissible to transfer personal data to any of the jurisdictions on the White List. If data users wish to rely on this exception to transfer personal data outside Hong Kong, it should therefore keep a close watch of the Commissioner's updating of the White List.

Section 33(2)(b) there is in force in that place "*any law which is substantially similar to, or serves the same purposes as*" the Ordinance

This exception is intended to address primarily the jurisdictions which have not been assessed by the Commissioner, rather than those jurisdictions which have been reviewed by the Commissioner and found inadequate for the purpose of inclusion in the White List.

If the intended recipient of the personal data is not located in a place on the Commissioner's White List, data users can still transfer personal data outside Hong Kong if they have reasonable grounds for believing that the place has in force "*any law which is substantially similar to, or serves the same purposes as*" the Ordinance. To satisfy such requirement, a data user is expected to undertake professional assessment and evaluation on its own of the data protection regime where the intended recipient is located. Such assessment should take into consideration various factors including the scope of application of the data privacy regime, the existence of equivalent provisions of the DPPs in the Ordinance, the data subjects' rights and redress, the level of compliance and the data transfer restrictions. Mere subjective belief will not suffice. A data user must be able to demonstrate its grounds of belief are reasonable if challenged. Reference may be made to the methodology adopted by the Commissioner in compiling the White List.

Since the assessment will require a sound knowledge of the foreign data protection regime, a data user should consult professionals or experts, and seek legal advice for such assessment. It should retain evidence (for example, the legal advice sought) of the assessment which it relies upon for its

[4] Either by repealing or amending the White List under section 33(4) of the Ordinance.

reasonable belief that the jurisdiction has in force "*any law which is substantially similar to, or serves the same purposes as*" the Ordinance. It is however unlikely to be accepted as 'reasonable' if the data user's assessment and belief is contrary to the determination by the Commissioner unless there are changes in the data protection regimes in such jurisdiction which have not yet been considered by the Commissioner at that time.

Section 33(2)(c) data subject's consent in writing to the transfer

Data users can transfer personal data outside Hong Kong if the data subject has consented to the transfer. Such consent needs to be expressly and voluntarily given **in writing** and has not been withdrawn. This more onerous requirement on the part of the data user to obtain consent is required since the giving of consent denotes the data subject's agreement for his personal data to be sent to a place with uncertain and perhaps substandard data privacy protection. The data subject should also be informed of the purpose of the transfer of the personal data and the consequences of providing such consent, i.e. his personal data may be subject to a lower standard of protection in another place to which his personal data may be transferred.

In order to obtain the data subject's written consent to the transfer, the data user should first provide the data subject with the information as to the places his personal data would be transferred to. Such information should be presented in a manner that is easily understandable and readable, and provided in a prominent place such as the Personal Information Collection Statement[5]. A separate tick box should be provided so that the data subject can signify his understanding and consent to the arrangement in writing.

Example of effective written consent:

For the purposes of providing [specify products and services] to you, we may transfer your name and contact details outside Hong Kong to our agents situated in [insert the list of jurisdictions], where there may not be in place data protection laws which are substantially similar to, or serve the same purposes as, the Personal Data (Privacy) Ordinance. That means your personal data may not be protected to the same or similar level in Hong Kong. Please indicate your consent by ticking the box below.

☐ I consent to the transfer of my personal data outside Hong Kong.

_____

Signature of the data subject
Name: xxx
Date: dd/mm/yyyy

Data users should retain evidence of the data subjects' written consent. Such written consent can be obtained by the data users themselves or by other persons (for example, third party data processor(s) acting on behalf of the data user). Where the written consent is obtained by other persons, the data users should ask for a copy of such written consent for their own record.

Section 33(2)(d) avoidance or mitigation of adverse action against the data subject

Data users can transfer personal data outside Hong Kong if they have reasonable grounds for believing that the transfer is for the avoidance or mitigation of adverse action against the data subject; it is not practicable to obtain the consent in writing of the data subject to that transfer; but if it was practicable, such consent would be given.

[5] It is a statement provided by a data user for the purpose of complying with the notification requirements under DPP1(3) of the Ordinance under which, for example, the data user is required to inform the data subject of the purpose of collecting his personal data and the class of transferees of such data.

This exception applies in special circumstances where the transfer is necessary for the protection of the interests of the data subject and it is not feasible for the data user to obtain the data subject's written consent before the transfer. Examples include the necessary transfer of personal data for the performance of a contract to which the data subject is a party and if the transfer is not proceeded with, the data subject would suffer significant financial loss.

This exemption has a narrow application. Data users have to prove their belief was reasonable by showing the relevant factual circumstances in justifying the transfer.

Section 33(2)(e) exemptions under Part VIII of the Ordinance

It is permissible to transfer personal data outside Hong Kong if one of the exemptions from the application of DPP3 under Part VIII of the Ordinance applies. The following are some of the relevant exemptions under Part VIII of the Ordinance that may be invoked by data users when transferring personal data outside Hong Kong:

- **Section 52** (domestic purposes): where personal data is held by an individual and is (i) concerned only with the management of his personal, family or household affairs; or (ii) so held only for recreational purposes;

- **Section 58** (crime, etc.): where personal data is transferred for the purpose of prevention or detection of crime[6] or for prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct or dishonesty or malpractice by persons, etc.;

- **Section 59** (health): the transfer of the identity, location and health data (physical and/or mental) of a data subject where non-disclosure may likely cause serious harm to the physical or mental health of the data subject or any other individual;

- **Section 60B** (legal proceedings): where the transfer of the personal data is required or authorised by Hong Kong law or in connection with any legal proceedings in Hong Kong or is required for establishing, exercising or defending legal rights in Hong Kong;

- **Section 61** (news): the transfer of personal data by a person to a data user whose business consists of a news activity and there is reasonable ground for that person to believe that the publication or broadcasting of the personal data is in the public interest;

- **Section 62** (statistics and research): where personal data is transferred for preparing statistics or carrying out research and the resulting statistics or research does not identify the data subjects; and

- **Section 63C** (emergency situation): where the transfer of the personal data is (i) to identify an individual who is reasonably suspected to be, or is involved in a life-threatening situation or (ii) to carry out emergency rescue operations, or provide emergency relief services.

Data users should refer to the relevant provisions in the Ordinance when relying on the above exemptions. Data users should be mindful that they bear the burden of proof to show that an exemption applies to the cross-border data transfer.

[6] "Crime" is defined under section 58(6) to mean an offence under the laws of Hong Kong; or if personal data is held or used in connection with legal or law enforcement cooperation between Hong Kong and a place outside Hong Kong, an offence under the laws of that place.

Section 33(2)(f) taken all reasonable precautions and exercised all due diligence that the personal data will not be handled in a manner that would be a contravention of the Ordinance

Another way to satisfy the cross-border transfer restriction is that the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data concerned is given equivalent protection to that provided for by the Ordinance ("**Due Diligence Requirement**"). Putting in place an enforceable contract between the parties to the transfer is one of the methods to satisfy this exception.

The Commissioner has prepared a set of recommended model data transfer clauses to assist data users to develop an enforceable contract for their cross-border transfer so as to satisfy this Due Diligence Requirement. The use of the recommended model data transfer clauses is explained in detail in the schedule to this Guidance.

Alternatively, data users may adopt non-contractual means to satisfy section 33(2)(f). Non-contractual oversight and auditing mechanisms may be adopted to monitor the transferees' compliance with the data protection requirements under the Ordinance. The relevant requirements are mainly the DPPs set out in Schedule 1 to the Ordinance. The transferees outside Hong Kong are required to observe the requirements under DPP2 to DPP6. DPP1 deals with collection of personal data and is therefore excluded. Data users may adopt the following measures:–

1. Data users are expected to transfer only to offshore entities which offer sufficient guarantees in respect of the technical competence and organisational measures governing the use and processing of personal data, and with a good track record on data protection.

2. Data users must be satisfied that the offshore entities have robust policies and procedure in place, including adequate training for their staff and effective security measures, to ensure that the personal data in their care is properly safeguarded at all times, is not kept for longer than necessary and will not be used for any purposes other than the purposes of the transfer. Data subjects' rights of access to and correction of their personal data should not be affected by reason of the transfer.

3. Where it is an intra-group transfer, data users are expected to have implemented adequate internal safeguards and policies as well as procedures which apply to the group as a whole. Such policies and procedures should reflect the requirements under the Ordinance.

4. Data users should also have the right to audit and inspect how the offshore entities use and process personal data, and exercise the right to audit and inspect on a regular basis to ensure compliance with the relevant requirements.

The above measures are not exhaustive and data users may take other steps to comply with the relevant requirements. When a complaint is received, the Commissioner will consider all the means engaged by a data user to protect personal data transferred to offshore entities to determine whether it has "taken all reasonable precautions and exercised all due diligence" to ensure that the personal data will be handled in the same manner as required by the Ordinance. Therefore, it is important that effective means are selected, implemented and properly documented.

PART 3: THE RECOMMENDED MODEL CLAUSES FOR THE PURPOSE OF SATISFYING THE DUE DILIGENCE REQUIREMENT UNDER SECTION 33(2)(F)

The Recommended Model Clauses serve as a recommendation for use by data users to satisfy the Due Diligence Requirement. It does not require strict adoption by parties in the cross-border transfer. Parties can insert additional clauses according to their business needs and/or commercial arrangements.

The Recommended Model Clauses are not intended to be the whole of the agreement between the transferring and receiving parties. They could be adapted by organisations in developing their own data transfer agreement or be incorporated into a wider outsourcing agreement which involves the transfer of personal data outside Hong Kong.

Where there are multiple transferees of the personal data, data users can adapt the Recommended Model Clauses into a multi-party agreement instead of having to enter into one agreement for each transferee. This is of particular relevance for multi-national corporations which adopt an intra-group centralised database allowing sharing of personal data across various jurisdictions.

Example:

The list of entities in and outside Hong Kong, i.e. the transferors and transferees, can be set out in a Schedule to the agreement. Each and every entity will execute and be bound by the terms of that single agreement. For subsequent entities, an adherence agreement could be adopted so that such entities will adopt the terms of the agreement.

Please refer to the schedule to this Guidance for the Recommended Model Clauses and the accompanying explanatory notes.

PART 4: PRACTICAL TIPS AND RECOMMENDED GOOD PRACTICES

Some key steps for data users to comply with section 33 are recommended below.

- **Review data transfer arrangement**

  Data users should review their existing data transfer arrangement to identify any cross-border transfer of personal data. Situations which may involve cross-border transfer of personal data include adoption of an offshore database system, outsourcing of data processing and/or storage functions and intra-group (members located outside Hong Kong) sharing of data. There are many other instances where transfer of personal data outside Hong Kong is involved. Data users should assess whether such activities are really necessary.

- **Control cross-border data flow activities**

  Data users should control activities that involve unintended or unnecessary cross-border data flow to avoid non-compliance with section 33. It is not uncommon for data users to exercise control through configuring their information technology system. One way is for international data users to structure the information technology system so that certain types of the data cannot be accessed or downloaded by their employees working in offices outside Hong Kong unless one of the exceptions under section 33(2) of the Ordinance has been complied with.

- **Check the White List and other exceptions**

  After identifying activities that require cross-border transfer of personal data, data users should then consider if any of the exceptions under section 33(2) applies. The first step will be to check the White List published by the Commissioner[7]. If

[7] See page 4 above for further explanation.

the White List exception does not apply, data users may consider relying on other exceptions, which include section 33(2)(c) by obtaining the data subject's written consent to the cross-border transfer and section 33(2)(f) by taking all reasonable precautions and exercised all due diligence to ensure equivalent protection to that provided under the Ordinance (e.g. by adopting an appropriate contract between the data user and the transferee)[8].

The Commissioner's prior consent is not required for transfers outside Hong Kong. The Commissioner is not the person from whom one should seek specific legal advice as to whether a particular destined place has in force any law which is substantially similar to, or serves the same purposes as, the Ordinance (except the White List published by the Commissioner). The Commissioner also does not offer case-specific legal advice as to how a valid contract should be signed between the parties. It is up to the data user to meet one of the exceptions under section 33(2) of the Ordinance.

- **Keep inventory of personal data**

  Another important aspect is for data users to keep an inventory of the personal data being transferred outside Hong Kong. Data users must always bear in mind that they remain responsible and accountable to the data subjects for possible contraventions of the requirements under the Ordinance. It is in their interests to monitor the data handling process of the transferees, to keep abreast of the whereabouts of the personal data and to assess the associated privacy risks. Also, data users should be transparent about their data handling policies and practices regarding any transfer of personal data outside Hong Kong.

- **Conduct regular audit and inspection**

  An effective monitoring tool for adequate and continued protection offered to the personal data transferred outside Hong Kong is regular audit and inspection on the transferees' operations to ascertain their compliance with their obligations under the data transfer agreement.

[8] See pages 4 to 7 above for more details.

Schedule:
Recommended Model Clauses

*Below sets out the Recommended Model Clauses which may be adapted and/or included in a data transfer agreement by parties who wish to transfer personal data outside Hong Kong in accordance with section 33(2)(f) of the Personal Data (Privacy) Ordinance (the "**Ordinance**"). Parties are advised to make adaptations or additions according to their own commercial needs. These clauses can be incorporated into a wider agreement such as an outsourcing agreement. The clauses may be adapted into a multi-party agreement.*

The terms used below have the same meanings given to them under the Ordinance. The parties are reminded to include clear definitions for the terms used in the data transfer agreement.

As the Recommended Model Clauses are drafted based on the requirements under the Ordinance, in order to achieve certainty on the application and enforcement of the Ordinance, the governing law of the agreement is the laws of Hong Kong. Resolution of disputes arising out of or relating to the agreement will be dealt with in Hong Kong for geographic proximity and convenience.

Set out below are the core clauses (see Section I) which are required to be included in the data transfer agreement. Apart from the core clauses, parties may wish to consider and include the additional clauses (see Section II) which aim at refining the parties' rights and obligations under a data transfer agreement but the absence of which will not render the contract inadequate for the purpose of satisfying the requirement under section 33(2)(f) of the Ordinance.

Please also see the accompanying explanatory notes to the Recommended Model Clauses at the end of this document.

Section (I) Core Clauses

1 Obligations of the Transferor

1.1 The Transferor represents and warrants to the Transferee that the personal data (as set out in Schedule 1 to this agreement) is lawfully transferred to the Transferee and that in accordance with data protection principle ("**DPP**") 3 in Schedule 1 to the Personal Data (Privacy) Ordinance (the "**Ordinance**"):

1.1.1 the personal data has been collected in accordance with DPP1 of the Ordinance;

1.1.2 all reasonably practicable steps have been taken to ensure its accuracy in accordance with DPP2 of the Ordinance;

1.1.3 the personal data has not been retained longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data is to be used; and

1.1.4 the transfer of the personal data is permitted by DPP3 of the Ordinance, as it is in line with the purpose for which the data was to be used at the time of the collection of the data, and where the data is to be used for a new purpose, the prescribed consent of the data subject has been obtained.

2 Obligations of the Transferee

2.1 The Transferee represents, warrants and undertakes the following:

2.1.1 The Transferee shall process or use the personal data for the purpose(s) as set out in Schedule 1 to this agreement to the exclusion of any other purpose. Where the transferred data is used for a new purpose, the Transferee shall obtain the prescribed consent of the data subject under the Ordinance.

2.1.2 The Transferee shall hold the personal data securely in accordance with the requirements of DPP4 of the Ordinance. It will have in place appropriate technical and organisational measures and standards as set out in Schedule 1 to this agreement to protect the personal data against unauthorised or accidental access, processing, erasure, loss or use.

2.1.3 The Transferee shall not retain the personal data longer than is necessary for the fulfillment of the purpose(s) (including any directly related purpose(s)) for which the personal data is to be used.

2.1.4 The Transferee shall use the personal data exclusively for the purposes set out in this agreement and shall not transfer or disclose, either free of charge or in return for any benefits, the personal data to any other person, except when it is compelled to do so under the applicable laws.

2.1.5 The Transferee shall immediately rectify, erase or return the personal data on receiving instructions to this effect from the Transferor. The Transferee undertakes in particular to rectify, erase or return all or part of the personal data if it appears that such measures are required by the requirements of the Ordinance.

2.1.6 The Transferee has and shall at all times have in place accessible documents which clearly specify its policies and practices in relation to personal data.

2.1.7 The Transferee shall ensure that data subjects have rights of access to and correction of their personal data in the same way as they would have had under the Ordinance.

2.1.8 The Transferee shall not disclose, transfer or allow access to the personal data to a third party data user or data processor ("Sub-transferee") located outside Hong Kong unless it has notified[1] the Transferor and:

2.1.8.1 the sub-transfer is made to a place that has in force any law which is substantially similar to, or serves the same purposes as the Ordinance[2];

2.1.8.2 such Sub-transferee becomes a signatory to this agreement or another written data transfer agreement which imposes the same obligations on it as are imposed on the Transferee under this clause 2; or

2.1.8.3 adopted all reasonable non-contractual measures and auditing mechanisms[3] to the reasonable satisfaction of the Transferor to monitor the Sub-transferee's compliance with the obligations under this clause 2 as if they are applicable to that Sub-transferee.

---

1 A Transferor may impose tighter control by prohibiting the Transferee from any further or onward transfer of personal data except with the Transferor's prior consent.

2 One way of finding out whether the law of the destined jurisdiction satisfies this requirement is to ascertain if it has already been included in the White List (being a list of jurisdictions which the Commissioner has determined to have in force "any law which is substantially similar to, or serves the same purposes as" the Ordinance under section 33(3) of the Ordinance).

3 Parties may specify the measures and mechanisms in Schedule 1.

2.1.9 Upon the Transferor's request, the Transferee shall submit its data processing facilities, policies and procedures, data files, documentation and any other relevant information for reviewing, auditing and/or certifying by the Transferor or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the Transferor, to ascertain compliance with its warranties and undertakings in this agreement.

3 Liability and indemnity

3.1 The Transferor and the Transferee shall be jointly and severally liable for any damage to the data subject arising out of or in connection with the transfer and any sub-transfer thereof of his/her personal data pursuant to this agreement.

3.2 Each party, to the extent to which it is liable, undertakes to hold harmless and indemnify the other party for any costs, charges, damages, payments, expenses or loss suffered or incurred for any breach resulting from its obligations under this agreement and for any fault or negligence arisen from the execution of this agreement.

3.3 The Transferee specifically undertakes to hold harmless and indemnify the Transferor for any costs, charges, damages, payments, expenses or loss suffered or incurred arising out of or in connection with the Transferee's engagement of any Sub-transferee and for any breach resulting from the obligations of any Sub-transferee under such data transfer agreement between the Transferee and that Sub-transferee.

4 Settlement of disputes

4.1 This agreement shall be governed, construed, and enforced in accordance with the laws of Hong Kong.

4.2 In the event of a dispute or claim brought by a data subject or the privacy enforcement authority concerning the processing of the personal data against either or both of the parties, the parties shall inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

5 Termination

5.1 Should the Transferee breach any of its obligations under this agreement, the Transferor may, without prejudice to any rights which it may have against the Transferee, terminate this agreement by serving a written notice to the Transferee.

5.2 The parties agree that on the termination of this agreement, the Transferee shall, upon the Transferor's request, return all the personal data transferred and the copies thereof to the Transferor or shall destroy all the personal data and certify to the Transferor that it has done so, unless applicable laws imposed upon the Transferee prevents it from returning or destroying all or part of the personal data transferred. In that case, the Transferee shall immediately so notify the Transferor and shall warrant that it will guarantee the confidentiality and integrity of the personal data transferred and will not process the personal data transferred anymore.

Schedule 1: Description of the Transfer

(To be completed by the parties as part of the agreement)

Transferor

The Transferor is (please specify briefly your activity relevant to the transfer):

Transferee

The Transferee is (please specify briefly your activity relevant to the transfer):

Data subjects

The personal data transferred concerns the following categories of data subjects:

Purposes of the transfer

The transfer is made for the following purposes:

Categories of data

The personal data transferred concerns the following categories of data:

Recipients

The personal data transferred may be disclosed only to the following recipients or categories of recipients (including Sub-transferees):

Security measures to be adopted by the Transferee

Please insert descriptions of the technical and organisational measures and standards to be adopted by the Transferee in relation to the security of the personal data:

Non-contractual measures and audit mechanisms to be adopted by the Transferee

Section (II) Additional Clauses

Set out below is a list of additional clauses which may be incorporated to assist data users to further enforce this agreement, but absence of which does not render the data transfer agreement inadequate to satisfy section 33(2)(f) of the Ordinance.

(i) Clauses relating to data subjects' third party rights under the Contracts (Rights of Third Parties) Ordinance[4]

6. Third Party Rights

6.1 The Transferor will make available, upon request, a copy of this agreement to data subjects unless the agreement contains confidential information, in which case the Transferor may remove such information.

6.2 The parties expressly agree that, pursuant to the Contracts (Rights of Third Parties) Ordinance, they intend to confer third party rights on the data subjects and the data subjects shall be entitled to enforce this clause 6, clause 1.1.2, 1.1.3, 1.1.4, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 2.1.7, 2.1.8, 3.1 and 4 of this agreement as if it was a party to this agreement in its own right. A data subject, who has suffered damage as a result of any breach of the obligations by the Transferee or any Sub-transferee under this agreement, or any breach of the obligations by any Sub-transferee under such data transfer agreement between the Transferee and that Sub-transferee, is entitled to receive compensation from the parties for the damage suffered. Notwithstanding the foregoing, the rights of both parties to this agreement to terminate, rescind or agree any variation, waiver or settlement under the agreement are not subject to the consent of the data subjects or any other person.

6.3 The parties agree that the data subject's rights pursuant to this agreement will not prejudice his substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

The clauses above are drafted for adaptation or adoption by parties who wish to confer third party rights on the data subjects after the commencement of the Contracts (Rights of Third Parties) Ordinance[5].

In conferring a right on the data subjects to enforce terms of the contract, the data subjects should be able to obtain a copy of the contract between the Transferor and the Transferee. The clauses should expressly provide that data subjects' rights under the agreement will not prejudice his/her substantive and procedural rights to seek remedies under other national or international law, for example, the Ordinance.

---

[4] Contracts (Rights of Third Parties) Ordinance has been published in the Gazette on 5 December 2014 (No. 49, Vol. 18 – Legal Supplement No. 1) as Ordinance No. 17 of 2014 (www.gld.gov.hk/egazette/pdf/ 20141849/es12014184917.pdf).

[5] Contracts (Rights of Third Parties) Ordinance will come into operation on a day to be appointed by the Secretary for Justice by notice published in the Gazette.

(ii) Additional obligations of the Transferee (to be inserted under clause 2 of the Recommended Model Clauses)

2.1.10 The Transferee has no reason to believe that there are currently in force any local laws that would have adverse effect on its warranties and/or undertakings as provided for under this agreement, and the Transferee shall notify the Transferor if it becomes aware of any such laws.

2.1.11 The Transferee has the legal capacity and the authority to give the warranties and/or undertaking in this agreement.

2.1.12 The Transferee shall inform promptly the Transferor of its inability to fulfill any of his obligations in this agreement.

2.1.13 The Transferee shall promptly notify the Transferor about any abnormalities or any loss, accidental or unauthorised access or processing, erasure or other use of the personal data.

2.1.14 The Transferee shall deal with promptly and properly all reasonable inquiries from the Transferor relating to the fulfillment of its obligations hereunder and the Transferee shall abide by the reasonable instructions or advice (if any) of the Transferor or any supervisory authority in this regard.

2.1.15 The Transferee shall ensure its staff who handle the personal data will carry out the security measures and obligations herein specified.

2.1.16 The Transferee shall identify a contact point within its organisation authorised to respond to the enquiries relating to the handling of the personal data, and shall cooperate with the Transferor, data subjects and relevant authorities concerning all enquiries within reasonable time.

Section (III) Explanatory Notes

(i) Data protection principles required to be observed by the Transferee[6]

In order that the data subjects may continue to enjoy the same or similar rights and protection as provided under the Ordinance for their personal data transferred outside of Hong Kong, the Transferor is required to include contractual terms in the agreement with the Transferee obligating the latter to observe the data protection principles ("**DPPs**") in Schedule 1 of the Ordinance.

The Transferee should be required by the agreement to comply with all DPPs with the exception of DPP1 which primarily deals with the collection of personal data unrelated to the Transferee. Observance of DPP2 is important to ensure the personal data is not retained by the Transferee after fulfillment of the purpose(s) for which the personal data is disclosed or transferred. DPP3 restricts the Transferee to use the personal data only for the purpose(s) as agreed under the agreement. The Transferee should also be required to observe DPP4 to ensure the security of personal data. The security and technical measures may vary depending on the actual circumstances. It is therefore advisable for the parties to decide and set out specific measures in Schedule 1.

DPP5 requires the Transferee to ensure transparency of its data protection policies and practices. The data subjects should have the same rights of access and correction of their personal data transferred outside Hong Kong, as such DPP6 should also be observed by the Transferee.

(ii) Sub-transfer[7]

It is not uncommon for the Transferee to subcontract data processing to another processor. In light of commercial reality and practicality, sub-transfer of personal data by the Transferee may be allowed subject to a certain degree of control being retained by the Transferor so that the personal data will still be subject to continued protection. Hence, the further or onward transfer of personal data by the Transferee should be effectively managed so that the purpose of section 33 will not be defeated or circumvented. The level of protection afforded to the personal data should not be reduced as a result of onward transfers. For this purpose, the sub-transfer of personal data by the Transferee is made subject to the fulfilment of any one of the pre-conditions under clauses 2.1.8.1 to 2.1.8.3 of the Recommended Model Clauses and upon notification to the Transferor. The primary objective is to ensure that the same obligations as the Transferee are imposed on any Sub-transferee, or that the law of the destined jurisdiction offers similar protection as under the Ordinance.

Where sub-transfer is in the contemplation of the parties at the time of entering into the Recommended Model Clauses, a multi-party agreement may be arranged so that the Sub-transferee enters into and becomes a signatory to the Recommended Model Clauses at the outset. Where sub-transfer happens after the conclusion of the Recommended Model Clauses, the Sub-transferee may either:–

(a) sign an adherence agreement to be bound by the terms of the Recommended Model Clauses; or

(b) enter into a separate agreement with the Transferee which imposes on it the same obligations as imposed on the Transferee under clause 2.

---

[6] Clauses 2.1.1 to 2.1.9 of the Recommended Model Clauses
[7] Clause 2.1.8 of the Recommended Model Clauses

For the non-contractual measures and auditing mechanisms to be adopted to ensure continued protection in a sub-transfer situation, parties are advised to specify the measures in greater detail in Schedule 1 to the Recommended Model Clauses.

(iii) Audit requirement for the transfer of personal data[8]

In order to ensure a Transferee fulfils its obligations under the data transfer agreement rather than pay lip service, clause 2.1.9 is included to enable the Transferor to require the Transferee to submit its data processing facilities and relevant documentation to the Transferor for the purpose of reviewing, auditing and ascertaining compliance with its obligations under the agreement. The Transferor is recommended to carry out such inspection before the commencement of transfer of personal data to the Transferee. Furthermore, regular audits and inspections after the transfer are important to safeguard personal data privacy protection and to discharge the transferor's duty under section 33(2)(f).

(iv) Liabilities of the parties[9]

It is essential that the data subject has recourse to compensation for the mishandling of his personal data transferred outside of Hong Kong. In case of any breach of the requirements under the Ordinance, given that it is difficult to claim against the Transferee which resides outside Hong Kong, the more viable option will be for the data subject to pursue his claims against the Transferor. In the absence of contractual third party rights under the current Hong Kong law[10], the data subject's redress against the Transferor and/or the Transferee may be founded under section 66 the Ordinance which allows data subject to claim compensation from data users for loss for breach of requirements under the Ordinance.

Under clause 3.1 of the Recommended Model Clauses, a data subject has recourse to compensation from both the Transferor and the Transferee, whose liability is joint and several, for mishandling of his personal data transferred outside Hong Kong.

Transferor's rights against the Transferee in breach are important for reducing the risks and liabilities since the Transferee resides outside of Hong Kong. In the event that the aggrieved data subjects make a claim for mishandling of their personal data transferred outside Hong Kong, or if the Commissioner takes enforcement actions, the Transferor, being a data user in Hong Kong, is ultimately liable for compensation and/or the penalties. The indemnity under clause 3.2 operates as a fair allocation of risk and liabilities between the Transferor and Transferee.

After the commencement of the Contracts (Rights of Third Parties) Ordinance, the parties may incorporate the additional clauses above relating to data subjects' third party rights which aim at conferring data subjects with the right to enforce the agreement even though they are non-parties to such agreement. Parties are advised to obtain legal advice in this regard.

(v) Resolution of disputes[11]

The resolution of disputes (between the parties or with the data subject) shall be dealt with in Hong Kong for geographic proximity and convenience. There is no restriction on the means of settlement of disputes. Parties are free to adopt mediation, arbitration and court proceedings in Hong Kong to resolve any disputes.

---

[8] Clause 2.1.9 of the Recommended Model Clauses
[9] Clause 3 of the Recommended Model Clauses
[10] Parties should keep in view of the Contracts (Rights of Third Parties) Ordinance, which is not yet commenced at the time of publication of this Guidance.
[11] Clause 4 of the Recommended Model Clauses

(vi) Termination[12]

The parties should address the Transferor's right for remedy in the event of breach by the Transferee of the agreement. The Recommended Model Clauses provide that the Transferor can terminate the agreement by serving a written notice to the Transferee in the event of a breach of the obligations by the Transferee. Alternatively, parties may provide in the agreement that in the event that the Transferee is in breach of its obligations under the agreement, the Transferor may temporarily suspend the transfer of personal data to the Transferee until the breach is rectified. If the breach is not rectified within a certain period of time (say 30 days), the Transferor may terminate the agreement. The Transferee is fully liable for its breach of obligations and the Transferor is indemnified by the Transferee for such breach.

On termination of the agreement, it is no longer required for the Transferee and/or any sub-transferee to retain the personal data transferred to them to fulfil the intended purposes, and such personal data should therefore be erased according to DPP2. Clause 5.2 of the Recommended Model Clauses provides that the Transferee and/or any sub-transferee are required to either return or destroy all the personal data transferred to them. Where the Transferee is prevented by any applicable laws from returning or destroying the personal data, the Transferee should be required to keep confidential, maintain integrity and cease any processing of the personal data.

[12] Clause 5 of the Recommended Model Clauses

Disclaimer

The information and suggestions provided in this publication are for general reference only. They do not serve as an exhaustive guide to the application of the Personal Data (Privacy) Ordinance. For a complete and definitive statement of the law, direct reference should be made to the Ordinance itself. The Privacy Commissioner makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information and suggestions set out in this publication. The information and suggestions provided will not affect the functions and powers conferred upon the Privacy Commissioner under the Ordinance.

First published in December 2014

PCPD.org.hk

Enquiry Hotline : **(852) 2827 2827**
Fax : **(852) 2877 7026**
Address : **12/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong**
Email : **enquiry@pcpd.org.hk**