MEKONG CLUB

FIGHTING THE BUSINESS OF SLAVERY

Financial Institutions Sharing Data Related to Human Trafficking

Financial Institutions Sharing Data Related to Human Trafficking

Sharing of information between financial institutions related to potential money laundering and human trafficking activities is essential in the fight against modern slavery. However, the laws covering personal data privacy, anti-money laundering, counter-terrorism and banking regulation are often seen as a barrier to any data sharing between banks.

In this paper, we seek to decode the key legislative requirements applicable in Hong Kong to facilitate a better understanding of what data can (and cannot) be shared and what limitations and exceptions apply.

1. TYPES OF DATA

CLIENT DATA – all the data that a bank holds on its client, including identification details, account information and transaction data.

Is Client Data also 'PERSONAL DATA' for the purposes of privacy law?

- YES – if it relates to an identifiable living individual
- NO – if it is sufficiently aggregated/anonymised that no individual is identifiable

CLIENT DATA

COMPANIES / INSTITUTIONS	INDIVIDUALS = PERSONAL DATA
• Identifiers – company details, legal form and proof of existence, company registration number, company accounts, tax records • Account information – types of account, account details, purpose of account • Transaction data – transfers, credit/debit card records, currency transaction reports	• Identifiers – name, address, phone number, email, passport/ ID number (including individual information of directors/officers of corporate clients) • Account information – types of account, account details, statements • Transaction data – transfers, credit/debit card records, ATM usage information

2. OVERVIEW OF LAWS

The banks owe an overriding duty of confidentiality to their clients under common law in Hong Kong. This means that information the banks hold on their clients can generally only be disclosed with the client's consent, or where it is compelled by law or required as part of legal proceedings involving the client, or where there is an overriding public interest in disclosure. Aside from the common law duty, there are a plethora of statutory obligations under privacy laws, counter-terrorism laws, anti-money laundering laws and banking regulations. The key ones are summarised in Appendix 1.

3. SHARING OF DATA – NOTICES / CONSENT / RESTRICTIONS

	PERSONAL DATA	OTHER CLIENT DATA	EXEMPTIONS
NOTICE - Is there a requirement to notify clients regarding sharing of data?	**YES –** At the time of collection of the data, the bank must notify clients regarding the purposes of collection and use of the data, as well as the classes of persons to whom the data may be disclosed. *(e.g. it should specify in its account opening forms or client contracts that data may be transferred to other banks for purposes of identifying human trafficking or other criminal operations).*	**NO –** There is no express notification obligation for other Client Data that is not personal data.	Under the Person Data (Privacy) Ordinance (PDPO), notice is not required if it would be likely to prejudice: - identification of an individual in a life-threatening situation, or notifying the individual's immediate family of such a situation; - carrying out emergency rescue operations or provision of emergency relief. (s63C PDPO)
CONSENT – Is consent required from clients for **on-shore** sharing of data (within HK)?	**NO –** Not for transfer within branches of same entity. **NO –** Not to the extent that the transfer falls within the notification requirement above (i.e. for the specified purpose and where the recipient is within the class of transferees notified to the client). **YES –** Consent required for transfer or disclosure to other entities that are not within the class of transferees notified to the client at the time of data collection.	**NO –** Not for transfer within branches of same entity. **YES –** Consent required for transfer or disclosure to third parties (including other group entities which are treated as third parties).	Consent not required for disclosure of any Client Data (including Personal Data) if: - the use of the Client Data is authorised or required by any law or court order in HK; - the Client Data needs to be used in connection with initiating or defending any legal proceedings in HK with respect to the client. Under PDPO, the following exemptions also apply (i.e. consent to disclosure of Personal Data not required): - prevention or detection of crime; - apprehension, prosecution or detention of offenders; - prevention, preclusion or remedying of unlawful conduct, dishonesty or malpractice. (s58 PDPO) The exemptions for notices (see section above re s63C PDPO) also apply here.

	PERSONAL DATA	OTHER CLIENT DATA	EXEMPTIONS
CONSENT – Is consent required from clients for **cross-border s**haring of data (i.e. outside HK)?	**NO –** Not to the extent that the transfer falls within the notification requirement above (i.e. for the specified purpose and where the recipient is within the class of transferees notified to the client). (s33 of PDPO still not in force) **YES –** Consent required for transfer or disclosure to other entities which were not within the class of transferees notified to the client at the time of data collection.	**YES –** A branch of the bank's same entity located outside HK would likely be regarded as a third party under common law duty of confidentiality. **YES –** *Consent required for transfer or disclosure to third parties outside of HK (including other group entities which are treated as third parties).*	The exemptions for **on-shore** transfers (see above) also apply here.

4. CONCLUSIONS

Although there are a number of legal constraints to sharing Client Data between financial institutions, there are several exemptions which may apply in circumstances related to identifying human trafficking or other criminal activity as listed above.

It is worth noting, however, that if the bank has sufficient evidence to establish that it can rely on one of the above exemptions, then it is likely that the obligation to submit a Suspicious Activity Report (SAR) under the drug-trafficking/serious-crimes legislation will be triggered, and once an SAR is submitted the bank cannot then share information relating to the SAR with other banks if such disclosure is likely to prejudice an ongoing investigation.

Also, if the suspected trafficking/money-laundering activities are being investigated by the Securities & Futures Commission (SFC), then the bank must not disclose any of the relevant Client Data to other banks if such disclosure would breach the 'secrecy obligation' under the Securities and Futures Ordinance (SFO). Although these restrictions may limit the ability to share 'live' information on specific cases, there is still a lot of useful general information that can be shared, provided it is anonymised (i.e. stripped of personal identifiers) such as:

- information on recent risk and crime trends;
- analytical data on methods, techniques, common typologies;
- information on identified threats;
- geographical vulnerabilities; and
- examples of investigation case studies.

The Financial Action Task Force (FATF)* has developed a number of guidelines and recommendations over the past few years, including Guidance on Private Sector Information Sharing**.

The Guidance highlights the need for more information sharing and better cooperation and engagement between the public and private sector. The report acknowledges that there is often a perceived conflict between AML/CTF laws which serve security and public interest goals on the one hand, and privacy laws which protect individual rights on the other. However, FATF notes that these should not be mutually exclusive and calls on governments and competent authorities (including financial regulators and data privacy authorities) to implement effective information sharing regimes and provide appropriate guidance to financial institutions, in particular regarding the extent to which sharing of personal data is permitted under public-interest/crime-prevention exemptions.

* FATF is an independent inter-governmental body working on policies and guidance to protect the global financial system against money laundering, terrorist financing and other criminal activities

** FATF (2017), Guidance on private sector information sharing, FATF, Paris www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-information-sharing.html

APPENDIX

1) What are the key applicable laws and regulations relating to the collection, processing, disclosure and transfer of data (collectively the "Laws")? Provide a summary of what each law or regulation covers.

(a) Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) (“AMLO”) (See particularly schedule 2 to AMLO)

The AMLO prescribes the customer due diligence and related record keeping requirements. It forms the legal basis for the bank to collect personal data including the copy and number of Hong Kong Identity Card (which would otherwise be subject to the restrictions prescribed by the "Code of Practice on the Identity Card Number and other Personal Identifiers" published by the Privacy Commissioner).

(b) Section 378 of the Securities and Futures Ordinance (Cap. 571) ("SFO") and Section 120 of the Banking Ordinance (Cap. 155) ("BO"), collectively the "Secrecy Obligation".

Section 378 of the SFO imposes a secrecy obligation on financial institutions, which prevents them from disclosing any information obtained in relation to any assistance provided to the Securities and Futures Commission ("SFC") (or any other specified person) in certain circumstances, including, for example, where they may be assisting the SFC in any investigation or inspection, or responding to any enquiry raised by the SFC.

It has a wide scope of application and the breach of which is a criminal offence. Section 120 of the BO also contains a statutory secrecy provision, but it is arguable that this only applies in relation to the Hong Kong Monetary Authority and its officers and agents.

(c) Common law duty of confidentiality

In general, a bank owes a duty of confidence to its clients subject to four qualifications:

(i) where disclosure is compelled by law;
(ii) where there is a duty to the public to disclose;
(iii) where the interests of the bank require disclosure (essentially for initiating or defending legal proceedings involving the client); and
(iv) where the disclosure is made by express or implied consent of the client.

(See: Tournier v National Provincial and Union Bank of England [1924] 1 KB 461)

(d) The Supervisory Policy Manuals ("SPM") published by the Hong Kong Monetary Authority ("HKMA")

See particularly:

(i) SPM SA-2 (Outsourcing);
(ii) SPM IC-6 (The sharing and use of consumer credit data through a credit reference agency); and
(iii) SPM CG-3 (Code of Conduct) (re s. 2.9 - Careful handling of customer data in accordance with common law customer confidentiality and the Personal Data (Privacy) Ordinance))

(e) HKMA circular re Customer Data Protection (14 October 2014)

HKMA reminds financial institutions of their obligations to ensure customer data is protected, and the need to report material breaches

(f) Guidelines on AMLO issued by HKMA and SFC.

These Guidelines explain the AMLO requirements in more detail.

(g) Code of Banking Practice issued jointly by the Hong Kong Association of Banks and the DTC Association, and endorsed by HKMA.

It sets out various obligations relating to confidentiality and privacy, including the requirement that financial institutions should:

(i) have in place appropriate control and protection mechanisms to protect customers' financial and personal information;
(ii) treat customers' banking affairs as confidential; and
(iii) comply with the PDPO.

(See particularly sections 2.6 and 8)

(h) SFC - Code of Conduct

Specific provisions concerning confidentiality apply to certain types of licensed persons:

(i) Licensed persons engaging in leveraged foreign exchange trading are expected to maintain confidentiality in respect of information relating to their clients. Except as required by law, such licensed person should not disclose to a third party any information relating to its clients without the client's explicit permission (Schedule 6, section 52).

(ii) Electronic trading systems, the e-trading systems should have system security to protect the confidentiality of information (Schedule 7).
(iii) For licensed or registered persons dealing in securities listed or traded on The Stock Exchange of Hong Kong Limited: Options contracts should contain statements that the licensed or registered person will keep information relating to the client's options account confidential, but may provide any such information to the SFC, the SEHK and Hong Kong Exchanges and Clearing Limited, as the case may be (Schedule 3).
(iv) SFC Fund Manager Code of Conduct

A Fund Manager should maintain proper procedures to ensure confidentiality of client information (Section 6.3).

(j) SFC – The Management, Supervision and Internal Control Guidelines for Person Licensed by or Registered with the SFC

It reinforces the duty of confidentiality of a licensed intermediary and emphasises the need for persons registered or licensed by the SFC to protect all confidential information in its possession, which would include any client's personal and financial information and price-sensitive information (Section IV).

(k) Drug Trafficking (Recovery of Proceeds) Ordinance (Cap.405) ("DTRPO") and of the Organised and Serious Crimes Ordinance (Cap.455) ("OSCO")

Regarding the disclosure of Suspicious Activity Reports ("SAR").

2) What type of data is protected by the Laws (e.g. personal data, client data, important data, etc.)?
Provide all relevant definitions, and identify which Law protects the relevant category of data.

Under common law, the bank's duty of confidentiality extends to all information in the bank's possession relating to the client (whether the client is an individual, a company or any other entity), including their accounts, affairs, dealings and transactions ("Client Data").

The PDPO protects the personal data of an individual irrespective of whether he/she is a client or customer of the bank (e.g. directors or officers of a corporate client, individual clients, potential clients, guarantors, employees, job applicants, beneficiaries, etc.). "Personal data" is: (i) any data relating directly or indirectly to a living individual; (ii) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (iii) in a form in which access to or processing of the data is practicable. Therefore, whilst the PDPO will not apply to any data relating to corporate clients, it will protect individual clients and the personal data of any directors, officers, etc., of the corporate clients. Personal data forms a subset of Client Data.

Information obtained in relation to any assistance provided by a bank with regard to an investigation, inspection or enquiry by the SFC is subject to the Secrecy Obligations.

3) Who is required to comply with the Laws (e.g. all financial institutions, data users, etc.)?

In relation to personal data, data users are obligated to comply with the PDPO. Data users are persons who control the collection, use, transfer, processing and retention of personal data. The PDPO only applies to data users that exercise such control from within Hong Kong (i.e. it does not have extra-territorial effect). As such, the PDPO will not apply to persons who control the collection, etc. of personal data from outside of Hong Kong, even if the data subjects are Hong Kong residents. Similarly, the PDPO will apply to persons who control the collection, etc. of personal data from within Hong Kong, even if the data subjects are outside Hong Kong.
The DTRPO and OSCO (see sub-paragraph (m) of question 1) applies to all persons (whether or not they are a financial institution).

The DTRPO and OSCO creates the offence of dealing with any property knowing or suspecting that it represents (in whole or in part) the proceeds of any drug trafficking or other indictable offence, and failing to report such knowledge or suspicion to the police or any other authorised officer (i.e. suspicious activity report or "SAR"). It is also an offence for any person who knows or suspects that an SAR has been made, to disclose to any other person any matter that is likely to prejudice any investigation that might be conducted in relation to the SAR.

With regard to the other Laws identified in question 1 (i.e. sub-paragraphs (c) to (l)) ("Banking Laws"), the requirements apply to institutions that are regulated by the HKMA and SFC, as applicable, e.g. financial institutions or persons licensed or registered with the SFC.

4) If the data is publicly available, is it still subject to the Laws?

Yes, publicly available information is still subject to the Laws.

For Client Data, if the information obtained from publicly available sources is integrated with and becomes inseparable from other Client Data, then they should be treated as Client Data and will be subject to the Banking Laws.

The PDPO applies to personal data collected from public sources. In particular, data users must comply with data protection principle ("DPP") 3 under the PDPO, i.e. personal data should only be used for the purposes for which it was collected (or a directly related purpose), unless the express and voluntary consent of the data subject (i.e. the individual who is the subject of the personal data) has been obtained.

Each public database / source must therefore be looked at to determine the original purpose of collection of the personal data, and the data should only be used for such purpose.

In August 2013, the Privacy Commissioner issued a Guidance on Use of Personal Data Obtained from the Public Domain . In general, the test to be applied as to whether or not a data user can use the personal data obtained from a public source is:

(a) whether the data user's use of the personal data falls within the original purpose of collection and use of the personal data (or a directly related purpose); and, if not

(b) whether a reasonable person in the data subject's shoes would find the re-use of the personal data by the data user as an unexpected, inappropriate or otherwise objectionable use – taking into account the context in which the data was collected and the sensitivity of the data.
Note that some public databases have clear restrictions on use of the data provided by them and there are other specific pieces of legislation that restrict and impose sanctions on the re-use of certain public data for other purposes. For example, use of information provided on the electoral register for a purpose other than one related to an election is an offence, and may result in a HK$5,000 fine and 6 months imprisonment.

Lastly, Section 64 of the PDPO makes it an offence for a third party to obtain personal data about an individual from a data user without the data user's consent, with an intent to use the personal data for gain or to cause loss to the data subject. It will be a defence for the third party to show that it reasonably believed that the data user had consented to the disclosure.
Secrecy Obligation

If it is public information, then the Secrecy Obligation shall not apply.

5) Are there any additional requirements or restrictions that apply to certain categories of data (e.g. sensitive data, national identification number, passport number, ethnicity, etc.)?

No, save in relation to information that is subject to the Secrecy Obligation or any SAR (see our response to question 1, sub-paragraph (m) and question 3).

Please note that the Privacy Commissioner has published guidelines regarding the collection and use of certain types of personal data that he considers to be particularly sensitive, and which need to be approached with caution.These include Hong Kong Identity Cards ("HKID") , consumer credit data and biometric data .

6) Does notice need to be provided to a person or organisation before their data is collected?

Client Data:
Under the Laws, there is no express notification obligation in relation to Client Data that does not constitute personal data, save in relation to any Client Data that will be disclosed as part of an outsourcing.

Under the SPM SA-2 published by the HKMA, in relation to any outsourcing, a bank should notify its customers in general terms of the possibility that their data may be outsourced. Specific notice to customers should be given of significant outsourcing initiatives, particularly where the outsourcing is to an overseas jurisdiction.

Personal Data:
Notice needs to be provided in relation to personal data that is collected directly from the individual. Under DPP 1(3) of the PDPO, a data user must take all practicable steps to ensure that the data subject is informed:

(a) on or before the collection of his/her personal data, of:

(i) the purpose for which the personal data are collected and to be used;

(ii) the classes of persons to whom the data may be disclosed;

(iii) (implicitly or explicitly) whether it is obligatory or voluntary for him/her to supply the data (and if it's obligatory, the consequences for him failing to supply the data); and

(b) on or before the first use of the personal data:

(i) his/her right to request access to and correction of the data; and

(ii) the name or job title and address of the individual who is to handle any such data access or correction request,

collectively referred to as the "Notification Obligation".

In practice, the Notification Obligation is complied with in the form of a personal information collection statement that is given to the individual at the time that they are first requested to provide their personal data, e.g. as part of the process for applying for a bank account.
Note that there are further notice requirements that apply in relation to the use of personal data for direct marketing purposes.

7) Is consent needed for the collection and use of data?

Client Data:
Consent is required if any Client Data (whether or not it constitutes personal data), will be transferred or disclosed to a third party. See our response to question 11 below.

Personal Data:
Under the PDPO, consent is only required if: the data user will be using the personal data for a new purpose, outside the scope of the original purpose for which it was collected (or a directly related purpose) (as notified to the data subject pursuant to our response to question 6 above) (DPP 3 of PDPO) -
(a) this includes transferring the personal data to a new set of recipients not covered by the original notice; or

(b) the personal data will be used or transferred for direct marketing purposes.

8) For what purpose can the collected data be used?

Client Data can be used for the purposes provided to the bank, and/or to fulfil the bank's obligations to the relevant client and/or to provide the services/facilities requested by the client.

Personal data can be used:
(a) for the purposes notified to the data subject pursuant to the Notification Obligation (see our response to question 6 above); or

(b) pursuant to the consent provided by the data subject (see our response to question 7 above); or in accordance with the exemptions set out in our response to question 10 below.

9) Are there any exemptions under the Laws to the requirement for notice?

Client Data:
See our response to question 12 below.

Personal Data:
The following exemptions apply to the Notification Obligation (note that these do not apply in relation to the notice required for direct marketing purposes):
Notice is not required if the personal data was not collected directly from the data subject (DPP 1(3) of PDPO);

(a) Notice is not required if the data is anonymised and it is not possible to re-identify the individual, as the data will not amount to personal data and will not be covered by the PDPO;

(b) Notice is not required if providing such notice would likely prejudice any of the following:

(i) identifying an individual who is reasonably suspected to be, or is, involved in a life threatening situation (Section 63C(1)(a) of PDPO);

(ii) informing an individuals' immediate family member or relevant persons of the individual's involvement in the life-threatening situation (Section 63C(1)(b) of PDPO);

(iii) the carrying out of emergency rescue operations or provision of emergency relief situations (Section 63C(1)(c) of PDPO); and

(iv) any of the purposes of use set out in the response to question 10 below.

9) Are there any exemptions under the Laws to the requirement for consent?

Client Data:
See our response to question 12 below.

Personal Data:
Yes. The following exemptions apply:

a) Consent is not required if the personal data will be used for the following purposes, and obtaining prior consent from the data subject will prejudice such purposes:

(i) the prevention or detection of crime;

(ii) the apprehension, prosecution or detention of offenders;

(iii) the assessment or collection of any tax or duty;

(iv) the prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, or dishonesty or malpractice, by persons;

(v) the prevention or preclusion of significant financial loss arising from any imprudent business practices or activities of persons or the unlawful or seriously improper conduct, or dishonesty or malpractice, by persons; and

(vi) ascertaining whether the character or activities of the data subject are likely to have a significantly adverse impact on anything to which the discharge of statutory functions by the data user relates;

(Section 58 of PDPO).

Note that reasonable suspicion or a mere or general assertion that the personal data will be used or disclosed for any of the purposes stated above (e.g. prevention or detection of a crime) may not be sufficient. The Privacy Commissioner takes the view that data users seeking to rely on section 58 of the PDPO have to obtain sufficient evidence to establish that the data are held or used for the specified purposes. This exemption and the associated defence are normally invoked in cases concerning requests (as opposed to a formal demand in the exercise of a legal or statutory power) for information by law enforcement agencies. Even in those situations, whilst noting the sensitive nature of most law enforcement operations, the Privacy Commissioner has advised data users to ask for the supply of more information in order for the data user to determine for itself whether one of exemptions apply, and to not simply rely on the request from the law enforcement agency.

Therefore in practice, to rely on the exemption or to invoke the defence under section 58 of the PDPO in any subsequent proceedings or complaint is not so straightforward.

Further, if the bank acquires sufficient evidence to establish that it can rely on one of the exemptions under section 58 of the PDPO (e.g. a crime may have been committed), then it is likely that its obligation to submit an SAR under DTRPO or OSCO (see sub-paragraph (m) of question 1) may arise, i.e. reporting to the police or other authorised officer if it knows or suspects that any property it is dealing with any represents (in whole or in part) the proceeds of any drug trafficking or other indictable offence.

Failing to report such knowledge or suspicion to the police or any other authorised officer amounts to an offence. Further, after submitting the SAR, the bank cannot then share any information relating to it with any other bank, if the disclosure is likely to prejudice any investigation that might be conducted in relation to the SAR.

(a) Consent is not required if the data is anonymised and it is not possible to re-identify the relevant individual, as the data will not amount to personal data and will not be covered by the PDPO;

(b) Consent is not required if the use of the personal data is authorised or required by or under any law or court order in Hong Kong (Section 60B(a) of the PDPO);

(c) Consent is not required if the personal data needs to be used in connection with any legal proceedings in Hong Kong or to establish, exercise or defend any legal rights in Hong Kong (Section 60B(b) and (c) of the PDPO);

(d) Consent is not required in relation to ascertaining whether the character or activities of the data subject are likely to have a significantly adverse impact on anything, which relates to the discharge of functions of a financial regulator for:

(i) protecting members of the public against financial loss arising from dishonesty, incompetence, malpractice or seriously improper conduct by persons concerned in the provision of banking, insurance, investment or other financial services; concerned in the management of companies, concerned in the administration of provident fund schemes registered under the Mandatory Provident Fund Schemes Ordinance; concerned in the management of occupational retirements schemes within the meaning of the Occupational Retirement Schemes Ordinance; or who are shareholders in companies; or the conduct of discharged or undischarged bankrupts;

(ii) for maintaining or promoting the general stability or effective working of any of the systems which provide any of the banking, insurance, investment or other financial services; or

(iii) a function specified for the purpose of this section by the government;

Note that financial regulator includes the HKMA, SFC and Insurance Authority, and other specified local regulators. The definition does not include foreign regulators.

(Section 58(3) of PDPO)

(a) Consent is not required if the personal data will be disclosed to a news agency or journalist, solely for the purposes of any news activity, and the discloser has reasonable grounds to believe that the publishing or broadcasting of the data is in the public interest (Section 61 of PDPO);

(b) Consent is not required if the personal data will be used solely for preparing statistics or carrying out research, and will not be used for any other purpose, and the results will not be made available in any form in which any data subjects may be identified (Section 62 of PDPO);

(c) Consent is not required if the personal data will be used in relation to the physical health, mental health, identity or location of a data subject, and prior consent would likely cause serious harm to the physical or mental health of the data subject or any other individual (Section 59 of PDPO);

(d) Consent is not required if the personal data will be disclosed by the data user for the purposes of due diligence related to a business transaction for the transfer of the business or property of or shares in the data user, or an amalgamation of the data user with another body, does not require the prior consent of the data subjects. However, this is subject to the primary purpose of the proposed business transaction not being the transfer, disclosure or provision for gain of personal data, and subject to other requirements imposed by the PDPO (Section 63B of PDPO);

(e) Consent is not required if obtaining consent would likely prejudice any of the following:

(i) identifying an individual who is reasonably suspected to be, or is, involved in a life threatening situation;

(ii) informing an individuals' immediate family member or relevant persons of the individual's involvement in the life-threatening situation; or

(iii) the carrying out of emergency rescue operations or provision of emergency relief situations;

(Section 63C of PDPO)

(f) Consent is not required if the personal data needs to be used for the purposes of ascertaining whether the character or activities of the data subject are likely to have a significantly adverse impact on anything to which the discharge of statutory functions by the data user relates (Section 58 of PDPO).

11) Under the Laws, what are the restrictions on the on-shore transfer or disclosure of data in the following circumstances?

11a) Between branch offices of the same entity;

No restriction. As they amount to the same entity, the bank is permitted to disclose Client Data (including personal data) to a branch of the bank's same entity in Hong Kong in connection with its business and its banker-client relationship with the client, without the specific consent of the client.
However, please note the Secrecy Obligation and the restriction on disclosing any information that might prejudice an ongoing investigation following the filing of a SAR (see our response to question 1, sub-paragraph (m) and question 3).

11b) Between different entities within the same group;

Restriction exists. An affiliate of the bank's same corporate group is regarded as a third party in the context of the common law duty of confidentiality and for the purposes of the PDPO. Accordingly, the bank is only permitted to disclose Client Data (including personal data) to an affiliate if one of the exemptions set out in our response to question 12 applies.
Note also the Secrecy Obligation and the restriction on disclosing any information that might prejudice an ongoing investigation following the filing of a SAR (see our response to question 1, sub-paragraph (m) and question 3).

11c) Between third parties that are unrelated and not in the same group;

Restriction exists. The bank is only permitted to disclose Client Data (including personal data) to a third party if one of the exemptions set out in our response to question 12 applies.
Note also the Secrecy Obligation and the restriction on disclosing any information that might prejudice an ongoing investigation following the filing of a SAR (see our response to question 1, sub-paragraph (m) and question 3).

12) If applicable, identify any exemptions to the restrictions on the on-shore transfer or disclosure of data in the following circumstances?

12a) Between branch offices of the same entity;

N/a

12b) Between different entities within the same group;

The bank can disclose the Client Data if:

(a) in so far as it amounts to personal data:

(i) the transfer is to a recipient that falls within one of the categories of transferees notified to the data subject pursuant to the Notification Obligation (see our response to question 6 above); or

(ii) the transfer is pursuant to the consent provided by the data subject (see our response to question 7 above); or

(iii) one of the exemptions set out in our response to question 10 above applies;

(b) it obtains the consent of the client;

(c) the use of the Client Data is authorised or required by or under any law or court order in Hong Kong;

(d) the Client Data needs to be used in connection with initiating or defending any legal proceedings in Hong Kong with respect to the client; and/or

(e) there is a duty to the public to disclose it.

With regard to any information that is subject to the Secrecy Obligation, it can only be disclosed with the express consent of the SFC, or if the information is already publicly available or is required to be disclosed in connection with a judicial proceeding, court order or applicable law. Regardless of the above exemptions, the disclosure of any information which might prejudice an ongoing investigation following the filing of a SAR amounts to an offence (see our response to question 3).

12c) Between third parties that are unrelated and not in the same group, including other financial institutions;

Yes. See our response to question 12(b) above.

13) Under the Laws, what are the restrictions on the cross-border transfer or disclosure of data in the following circumstances?

13a) Between branch offices of the same entity;

Restriction exists. A branch of the bank's same entity outside of Hong Kong is effectively regarded as a third party in the context of the common law duty of confidentiality. Whilst each case is decided on their own facts, the general case law supports the principle that there should not be unlimited disclosure or transfer of client data by a Hong Kong branch of a foreign bank to the head office or any branch outside of Hong Kong. Given that the common law duty is contractual in nature, the client's intention and reasonable expectations are relevant. If the client intends and expects to maintain his account with the branch in Hong Kong (and not with the head office or any branch outside of Hong Kong, and other circumstances are consistent with that, e.g. the client account documents are governed by Hong Kong law), disclosure of the client data without the client's consent by the Hong Kong branch to the head office or any branch outside of Hong Kong (even if they are the same entity), for any reason or purpose unrelated to Hong Kong branch's provision of the agreed services to the customer in the ordinary course of business, may be regarded as breach of the bank's common law duty. Accordingly, the bank is permitted to disclose client data if one of the exemptions apply.

See F.D.C. Co Ltd v Chase Manhattan Bank, N.A. [1990] 1 H.K.L.R. 277.
Note also the Secrecy Obligation and the restriction on disclosing any information that might prejudice an ongoing investigation following the filing of a SAR (see our response to question 1, sub-paragraph (m) and question 3).

13b) Between different entities within the same group;

Restriction exists. An affiliate of the bank's same corporate group is regarded as a third party in the context of the common law duty of confidentiality and for the purposes of the PDPO. Accordingly, the bank is only permitted to disclose Client Data (including personal data) to an affiliate if one of the exemptions set out in our response to question 12 applies.
Note also the Secrecy Obligation and the restriction on disclosing any information that might prejudice an ongoing investigation following the filing of a SAR (see our response to question 1, sub-paragraph (m) and question 3).

13c) Between third parties that are unrelated and not in the same group, including other financial institutions;

Restriction exists. The bank is only permitted to disclose Client Data (including personal data) to a third party if one of the exemptions set out in our response to question 12 applies.
Note also the Secrecy Obligation and the restriction on disclosing any information that might prejudice an ongoing investigation following the filing of a SAR (see our response to question 1, sub-paragraph (m) and question 3).

14) If applicable, identify any exemptions to the restrictions on the cross-border transfer or disclosure of data in the following circumstances?

14a) Between branch offices of the same entity;

The bank can disclose the Client Data if:

(a) in so far as it amounts to personal data:

(i) the transfer is to a recipient that falls within one of the categories of transferees notified to the data subject pursuant to the Notification Obligation (see our response to question 6 above); or

(ii) the transfer is pursuant to the consent provided by the data subject (see our response to question 7 above); or

(iii) one of the exemptions set out in our response to question 10 above applies;

(b) it obtains the consent of the client;

(c) the use of the Client Data is authorised or required by or under any law or court order in Hong Kong;

(d) the Client Data needs to be used in connection with initiating or defending any legal proceedings in Hong Kong with respect to the client; and

(e) there is a duty to the public to disclose it.

With regard to any information that is subject to the Secrecy Obligation, it can only be disclosed with the express consent of the SFC, or if the information is already publicly available or is required to be disclosed in connection with a judicial proceeding, court order or applicable law. Regardless of the above exemptions, the disclosure of any information which might prejudice an ongoing investigation following the filing of a SAR amounts to an offence (see our response to question 3).

Note that under the Laws, there are no specific restrictions currently in force in respect of the transfer of personal data outside of Hong Kong. Section 33 of the PDPO, which imposes restrictions on the transfer of personal data outside of Hong Kong, has been on the statute books since the PDPO was enacted in 1996. However, Section 33 has yet to come into force. When it does come into operation, Section 33 of the PDPO shall prohibit the transfer of personal data from Hong Kong to another jurisdiction, except in one or more specified circumstances. Even though Section 33 is not yet in operation, data users are still required to comply with the Notification Obligation in relation to the transfer of personal data to any third party (see our response to question 6 and question 7).

14b) Between different entities within the same group;

See our response to question 14(a) above.

14c) Between third parties that are unrelated and not in the same group, including other financial institutions;

See our response to question 14(a) above.

15) Are there any data localisation requirements under the Laws, which require the on-shore storage of data?

No.

16) If applicable, are there any exemptions to the data localisation requirements?

N/a.

17) Can data be shared amongst financial institutions (whether on-shore or off-shore) for the purposes of identifying any human trafficking operations or other crimes (e.g. money laundering)? In particular, can it be shared between:

There is overlap between the Laws and the different restrictions and requirements. As such, we would recommend that Client Data (including personal data) only be transferred where the consent of the client has been obtained.

Even if such consent has been obtained, the bank must:

(a) be able to justify why it is appropriate to disclose the data to other banks rather than/in addition to making disclosure to relevant law enforcement agencies;

(b) only share data that is necessary for the relevant purpose, and is not excessive (e.g. consider whether it is necessary to share all personal data on a client); and

(c) implement security measures to prevent any misuse or mishandling of shared data.

If the suspected human trafficking operations and/or money laundering activities have been reported to the authorities and/or are being investigated by the SFC, then the bank must not disclose any Client Data or other information to any other banks, any entities within its group or any other third party, if such would amount to a breach of its Secrecy Obligation or may prejudice any ongoing investigation. Otherwise, the bank may be guilty of an offence.

17a) Between branch offices of the same entity;

Yes, so long as the transfer is within the same entity and it involves an onshore disclosure of data. If it involves a cross-border transfer of data, then the data cannot be shared, unless the terms of the account opening forms or client contracts, etc. of the bank expressly allow the bank to transfer the Client Data to other branch offices for the purposes of identifying any human trafficking or criminal operations.

Even if the bank can disclose any data to its branch offices, it must at all times ensure that it complies with any Secrecy Obligations and/or that the disclosure does not prejudice any ongoing investigation following the filing of a SAR (see our response to question 3).

17b) Between different entities within the same group;

No, unless the terms of the account opening forms or client contracts, etc. of the bank expressly allow the bank to transfer the Client Data to other entities within the same group for the purposes of identifying any human trafficking or criminal operations. Even if such consent has been obtained, the bank needs to ensure it complies with any Secrecy Obligations and/or that the disclosure does not prejudice any ongoing investigation following the filing of a SAR (see our response to question 3).

17c) Between third parties that are unrelated and not in the same group;

No, unless the terms of the account opening forms or client contracts, etc. of the bank expressly allow the bank to transfer the Client Data to other third parties for the purposes of identifying any human trafficking or criminal operations. Even if such consent has been obtained, the bank needs to ensure it complies with any Secrecy Obligations and/or that the disclosure does not prejudice any ongoing investigation following the filing of a SAR (see our response to question 3).

info@themekongclub.org

www.themekongclub.org