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

info@themekongclub.org

www.themekongclub.org