



香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

(13)

專員用箋 From the desk of the Commissioner

Your Ref: RH/AL/kw/SG141
Our Ref: PCPD(O) 45/85/115 (200802494)

14 August 2008

The Law Society of Hong Kong
3/F, Wing On House
71 Des Voeux Road Central
Hong Kong.

(Attn.: Mr. Raymond HO, Secretary General)

Dear Sir,

**Personal Data (Privacy) Ordinance (“the Ordinance”)
Practice Direction P
Guidelines on Anti-Money Laundering and Terrorist Financing**

Referring to the endorsement given by me on 26 June 2008 pursuant to Clause 3.2.2.2 of the Code of Practice on the Identity Card Number and other Personal Identifiers (“the PI Code”) on collection of copies of identification documents of clients by your members under paragraph 86 of the captioned Practice Direction P, I note with concern the misunderstanding and confusion that some solicitors have on the situations under which copies of clients’ identification documents shall be collected since the coming into effect of Practice Direction P on 1 July 2008. I find it necessary to state clearly my rationale for giving the endorsement and its proper scope of application.

The basis of Practice Direction P

As I understand it, the Practice Direction P was issued to facilitate your members' compliance with the 40 Recommendations and 9 Special Recommendations ("the Recommendations") issued by the Financial Action Task Force ("FATF") to counter money laundering and terrorist financing activities, which extend to cover Designated Non-Financial Business and Professions ("DNFBP"), including solicitors. Recommendations 5 and 12 quoted by you form the basis of Practice Direction P. Recommendation 5, which primarily targets financial institutions, stipulate that they should undertake customer due diligence including identifying and verifying the identity of their customers when, establishing business relationship and carrying out occasional transactions, etc. Sub-paragraph (d) of Recommendation 12 is more specific in applying to DNFBP such as lawyers, notaries, legal professionals and accountants to carry out customer due diligence when carrying out transactions concerning the following activities :

- buying and selling of real estate;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organization of contributions for the creation, operation or management of companies;
- creation, operation or management of legal persons or arrangements; and buying and selling of business entities.

The above examples illustrate the situations when risks of money laundering and terrorist financing arise so that DNFBP should be cautious in conducting clients' due diligence before putting through these transactions. The common characteristic of these examples is that it directly or indirectly has a monetary element.

A risk-based approach

It is patently clear from the following provisions of Practice Direction P that a risk-based approach is to be adopted by the solicitors:

- (i) Clause (31) : that law firms should take a risk-based approach in establishing policies and procedures to combat

- money laundering and terrorist financing;
- (ii) Clause (55) : money laundering is transaction(s) effected with the aim to conceal or change the identity of **criminal proceeds**, so that the **money**, after such processing, will appear to have originated from a legitimate source.
 - (iii) Clause (56) : the definition of “money laundering activities” found in the Securities and Futures Ordinance clearly denotes a monetary element;
 - (iv) Clause 102 : a law firm is to conduct client due diligence when acting for a client “*in any **financial transaction** or any activity involving custody, management or transfer of **funds or assets**, to obtain information on the business relationship between the client and other interested parties to the transaction(s)*”; and
 - (v) Annex 4 sets out examples of suspicious transaction indicators and risk areas which necessarily involve the handling of **money, assets, property, proceeds, funds**, etc.

Solicitors have to assess in each case the risks of money laundering activities and terrorist financing by taking into account relevant factors such as the type of client, the business relationship in issue, the transaction involved, etc. The extent of client’s due diligence to be conducted should be commensurate with the existence and degree of the risk so assessed.

The general scenario of verifying client’s identity by solicitors

There is some confusion among your members that the endorsement given by me has the effect of changing the current practice of verifying client’s identity by making it mandatory for copies of ID cards of client to be retained. I therefore consider it necessary to make the following clarifications. Generally when solicitor-client relationship is entered into and instructions of client are taken, a solicitor is likely to collect personal data from his client which may include his identifying particulars. The extent and mode of collection in any particular case is a matter of professional judgment on the part of the solicitors insofar as only necessary, adequate but not excessive personal data are collected for the intended purpose of the retainer. Thus, a solicitor may find it sufficient merely to inspect the identity card of his client without

recording the particulars, such as name and ID number. Where the data are not collected in recorded form, the Ordinance does not apply.

In some cases, a solicitor may just collect the name and ID number of his client without making a copy of his ID card for retention. Section II of the PI Code sets out the circumstances under which ID number can be collected, such as when authorized by law or where the use is necessary, e.g. for insertion into a document to evidence any legal or equitable right or interest or any person.

When a copy of the client's ID card is collected, the solicitor should comply with Part III of the PI Code which is explained below.

The collection of copy of an identity card under the PI Code

The PI Code in Clauses 3.1 to 3.4 set out the limited circumstances under which identity card copies can be collected. A data user has to justify that valid ground(s) for collection of the copies of the identification documents as stated in the PI Code apply in the particular circumstances of the case that renders collection necessary, for instance, for prevention and detection of crime or prevention, preclusion or remedying unlawful or seriously improper conduct, or dishonesty or malpractice of persons (i.e. the purposes mentioned in section 58(1) of the Ordinance). A typical example is where a copy of the identity card of an individual vendor in a conveyancing transaction is collected to verify his identity to guard against fraud committed by impostor. Other than the situation covered by Clause 3.2.2.2 (see paragraph below), no endorsement by the Privacy Commissioner for Personal Data ("the Commissioner") is required for collection of copies of identity cards.

The scope of endorsement given by the Commissioner under Clause 3.2.2.2 of the PI Code

Pursuant to Clause 3.2.2.2, the Commissioner may endorse the act or practice of collection of copies of the identity cards in order for a data user to comply with such requirement as contained in any code, rules, regulations or guidelines applicable to the data user and issued by a regulatory or professional body. Without prejudice to the application of the other situations mentioned

in the PI Code above and without affecting the current practice commonly carried out by solicitors by inspecting the identification document or collecting the number of it, your application for endorsement made under Clause 3.2.2.2 is a only matter of convenience confining to certain situations for enabling your members to collect copies of the identity cards of the clients to be retained for a number of years stipulated in paragraph 86 of Practice Direction P in order to comply with the Recommendations.

Collection of copies of the clients' identification documents has to comply with Data Protection Principle ("DPP") 1 of the Ordinance in that only necessary, adequate but not excessive personal data shall be collected for the lawful functions and activities of the data user. Hence, where copies of identification documents of the clients are to be collected in compliance with the Recommendations and Practice Direction P, the collection must be justified to be necessary when there is a risk of money laundering or terrorist financing activities.

In many cases handled by a law firm, no money transactions are involved, e.g. provision of legal advice, participation in litigation, preparation of will, etc. The collection of copies of identification documents on a general basis when there is apparently no or low risk of such unlawful activities can hardly be justified to be necessary under DPP1.

In giving the endorsement aforesaid and having regard to the intention behind Practice Direction P, I was mindful of the fact that the situations contemplated under Paragraph 1 of Section A of Practice Direction P (i.e. Table of mandatory requirements) are predicated upon the existence of a risk of money laundering and terrorist financing activities that necessitates the collection of copy of identification documents for records. Hence, the collection of copies of the individual client's identification documents as set out in paragraph 86 of Practice Direction P should be read and apply when this pre-condition is satisfied. The mere existence of a solicitor-client relationship does not render the collection of copy of identification documents necessary on a general basis.

The situations contemplated by Paragraph 1 of Section A of Practice Direction P require that steps be taken to obtain basic information on the identity of the client in all cases when (i) establishing business relationship or (ii) carrying out occasional transactions. The Practice Direction does not

explain what constitute “business relationship” and “occasional transaction”. By drawing reference to the Anti-Money Laundering Practice Note issued by the Law Society of England and Wales on 22 February 2008, it is noted that these terms are clearly defined. “Business relationship”¹ denotes a relationship that has an element of duration and “occasional transaction”² refers to a monetary transaction exceeding a certain amount. This has reinforced my view that the mandatory requirements in Practice Direction P are not to be interpreted out of context without giving due consideration to the risk of money laundering and terrorist financing activities. Such risk may arise when a solicitor represents his client to enter into business relationship with an element of duration (such as with a third party) or where he acts for a client in occasional monetary transactions.

I hope this letter will clarify the scope of the endorsement given by me under Clause 3.2.2.2 of the PI Code. I consider it desirable that your members’ attention be brought to the contents of this letter in order to ease their concerns and wish to know whether you are agreeable to this being done.

Yours faithfully,

(Roderick B. WOO)
Privacy Commissioner for Personal Data

¹ The term is defined to mean “ a business, professional or commercial relationship between a relevant person and a customer, which is expected by the relevant person at the time when contact is established to have an element of duration”.

² The term is defined to mean “a transaction (carried out other than as part of a business relationship) amounting to 15,000 euros or more, whether the transaction is carried out in a single operation or several operations which appear to be linked”.