

June 2022

General Questions Raised to Privacy Commissioner

Introduction

In April 2018, under the 'Money Laundering and Terrorist Financing Risk Assessment Report'¹ (**Report**), submitted by the Government to the Financial Action Task Force (**FTAF**)², the position of members of the Institute in the international anti-money laundering and counter financing of terrorism (**AML/CFT**) fight was recognised. Specifically, under Chapter 6 of the Report, it was noted that many individuals and practitioners practising in the trust or company service providers (**TCSP**) sector are members of the Institute and occupy senior management positions in the corporations where they practice. Further, the Institute has provided related training, established voluntary

guidelines, and entered the AML/CFT Charter with leading TCSP firms to support the Institute's efforts in promoting AML/CFT standards and practices for the TCSP sector.

The Report was published a month before the coming into force of the licensing regime by the Government where the Companies Registrar at the time, Ms Ada Chung FCG HKFCG, an Institute Fellow, became the regulator for the TCSP sector. This was done through amendments to the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) (**AMLO**) to establish a civil regulatory regime. TCSPs were required to have policies to engage in conducting customer due diligence, including identifying ultimate

1 https://www.fstb.gov.hk/fsb/aml/en/doc/hk-risk-assessment-report_e.pdf

2 <https://www.fatf-gafi.org/>

Gratitude is expressed to the following persons for input to the guidance:

- Ms Ada Chung FCG HKFCG, Privacy Commissioner for Personal Data; and Ms Clemence Wong, Office of the Privacy Commissioner for Personal Data, Hong Kong
- Mr Ernest Lee FCG HKFCG(PE), Institute President, and Technical Partner, Deloitte China
- Mrs Natalia Seng FCG HKFCG, Institute Past President
- Mr Mohan Datwani FCG HKFCG(PE), Institute Deputy Chief Executive as the author of the guidance

If you have any comments and/or suggestions relating to any thought leadership matters, please contact Mohan Datwani at mohan.datwani@hkcg.org.hk

beneficial ownership (**UBO**) of their clients, aside from other regulatory compliance matters. The Companies Registrar established the 'Registry for Trust and Company Service Providers' (**TCSP Registry**) with day-to-day oversight of her regulatory functions.

As part of the identification of the UBO and other customers' due diligence required of licensed TCSPs, they may come into contact with third party information. This brings about privacy concerns including where there is a need to obtain third party data. The related issue is how long the data can be kept. It is fortuitous that Ada Chung is now also the Privacy Commissioner under the Personal Data (Privacy) Ordinance (Cap. 486) as well as the HKCGI Prize Awardee. The Institute now shares some general questions raised to the Privacy Commissioner and her team's kind responses. These contain important regulatory views for the TCSP sector as well as for the governance professional as keeper of significant controllers' registers (**SCRs**) for Hong Kong incorporated companies containing the related UBO information.

Questions raised to Privacy Commissioner

The Institute noted that for European Union's TCSP customers, under the General Data Protection Regulation (GDPR), there is the requirement to remove their private data after a certain period, with a need to notify them of the removal. The Institute wonders if there is an obligation to follow suit in Hong Kong for personal data only to be kept for a reasonable period. Specifically, and problematic is how long to keep personal data obtained from customers obtained during know our client (**KYC**) due diligence?

Further, for SCRs, there could be the situation of Hong Kong companies holding onto third party data of their UBOs. Is consent necessary? Also, similarly, how long should the data be kept and removed, say after a UBO and/or intermediary chain cease to be registrable on an SCR? These are not data of shareholders where there are statutory requirements for retaining filings.

Answers provided

The Office of the Privacy Commissioner for Personal Data (**PCPD**) kindly provided the following answers to the questions raised by the Institute relevant to TCSPs and keepers of SCRs of Hong Kong incorporated companies.

In respect of the questions raised which are primarily related to the retention of personal data, please find the relevant observations from the perspective of the Personal Data (Privacy) Ordinance (Cap. 486) (the "**PDPO**") as set out below for your kind consideration.

Personal Data Retention

1. Data Protection Principle ("**DPP**") 2(2) in Schedule 1 of the PDPO stipulates that all practicable steps must be taken to ensure that personal data shall not be retained longer than is necessary for the fulfilment of the purposes (including any directly related purposes) for which the data is or is to be used. It is noted that there is a similar storage limitation principle under the GDPR. DPP2(2) also accords with section 26(1) of the PDPO which requires a data user to take all practicable steps to erase personal data held by the data user where the data is no longer necessary for the purposes (including any directly related purposes) for which the data was used, unless it is prohibited by law, or in the public interest not to do so.
2. Whilst the PDPO does not specify any required limit of duration of personal data retention, as a good practice, data users are encouraged to (i) set a retention period for the personal data concerned, having regard to their operational needs; and (ii) erase the personal data concerned as appropriate.

Personal Data Obtained in KYC Due Diligence

3. It follows that the personal data obtained from customers during KYC due diligence should not be retained longer than is necessary for the fulfilment of the intended purpose(s) of use. The duration of the retention period will depend on the circumstances of each case, such as the nature of the businesses, the duration of the business relationships concerned, etc. In general, it will unlikely raise compliance issues so long as there is reasonable justification as to the retention period set for the purpose(s) intended to be achieved for the collection of the personal data (such as for facilitating the ongoing management of relationships with customers, etc.).

Significant Controllers Registers (“SCRs”)

4. In respect of SCRs and so far as personal data of individuals is concerned, it is noted that a company is required to issue a notice to an individual, whom the company knows or has reasonable cause to believe to be a registrable person, to confirm and/or request the provision of personal particulars as required for the purpose of identifying the significant controllers of the company.
5. According to DPP3 of the PDPO, prescribed consent of an individual data subject is required if the personal data previously collected is to be used for a new purpose, unless where any of the statutory exemptions in Part 8 of the PDPO applies. A new purpose means a purpose other than the purpose (or a directly related purpose) for which the data was to be used at the time of collection of the data. In this context, no prescribed consent is required to be sought from the data subjects concerned in general so long as the purpose of using their respective personal data (including making the same available in the SCRs for inspection) does not constitute a new purpose, in particular

when they have been made aware of the said purpose by way of notice.

6. As regards paragraph 5 on the question of consent, it is noteworthy that where the use of personal data is required or authorized by or under any enactment, or any rule of law, such use is exempt from the limitation of use principle as specified in DPP3 (section 60B of the PDPO).
7. Regarding retention of the personal data concerned, the requirements of DPP2(2) and section 26(1) of the PDPO as elaborated in paragraph 1 hereinabove shall apply likewise. It appears that it will no longer be necessary to retain the personal data of the significant controller concerned in an SCR, once he/she ceases to be registrable thereon. Nevertheless, this will depend on the circumstances of each case (such as the retention requirements imposed by any other applicable laws, etc.), to determine the reasonableness of the retention period.

Conclusion

Please kindly take time to read the DPPs referred to under this Guidance Note. Also, to recap, as noted by the PCPD:

1. Whilst the PDPO does not specify any required limit of duration of personal data retention, as a good practice, data users are encouraged to:
 - a. set a retention period for the personal data concerned, having regard to their operational needs; and
 - b. erase the personal data concerned as appropriate.
2. Accordingly, please ensure that these matters are considered and that there should be reasonable justifications as to the retention period set

for the purpose(s) intended to be achieved for the collection of the personal data (such as for facilitating the ongoing management of relationships with customers, etc.).

3. In addition, where the use of personal data is required or authorized by or under any enactment, or any rule of law, such use is exempt from the

limitation of use principle as specified in DPP3 (section 60B of the PDPO).

The above is not intended to provide any specific advice and each case may need to be considered with reference to the relevant facts or professional advice, as necessary.