PCPD's submission in response to the Consultation Paper on Implementation of Mandatory Reference Checking Scheme to Address the "Rolling Bad Apples" Phenomenon

This submission is made by the Privacy Commissioner for Personal Data ("PCPD") in response to the consultation paper published by the Hong Kong Monetary Authority ("HKMA") on implementation of mandatory reference checking scheme to address the "Rolling Bad Apples" phenomenon ("Consultation Paper") in May 2020.

2 As the regulator to oversee compliance with the Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO"), the PCPD offers comments on selected matters mentioned in the Consultation Paper that may have a personal data privacy protection angle.

Background

3 The HKMA is working with the banking industry in Hong Kong to address a phenomenon called the "Rolling Bad Apples" ("RBA"). In gist, RBA refers to individuals who engage in misconduct during their employment in the institutions but are able to obtain subsequent employment elsewhere without disclosing their earlier misconduct to the new employer.

4 To tackle the RBA phenomenon, the HKMA proposes to establish a common protocol for mandatory reference checking with an aim to help enhancing the disclosure of employment history of prospective employee to cover conduct specific information before a hiring decision is made by the bank ("MRC Scheme").

5 In short, it is proposed that a bank in Hong Kong will be required to conduct reference checking with the previous employer(s) and the current employer who are banks in Hong Kong for a prospective employee applying for specified positions. Apart from the general employment information such as employment duration, position held, description of role and the reason for cessation, specific information regarding the conduct of the prospective employee will be covered. The specific information would include: (i) breach of legal or regulatory requirements relating to the Banking Ordinance, Insurance Ordinance, Mandatory Provident Fund Schemes Ordinance and Securities and Futures Ordinance; (ii) incidents related to honesty, integrity or matters of similar nature; (iii) misconduct reports filed with the HKMA; (iv) internal or external disciplinary actions arising from conduct matters; and (v) any other additional information relevant to the fit and proper assessment.

General Comments

6 The overriding principle is that any measures that may intrude personal data privacy should be necessary, appropriate and proportionate to the purposes to be achieved.

7 The PCPD fully appreciates the adverse consequences of RBA and the operational, reputational and financial risks that would be brought to the recruiting banks as depicted in the Consultation Paper. The limitations of the existing mechanism (which is not aimed specifically at tackling the RBA phenomenon) has also given rise to a pressing need for the proposed MRC Scheme.

8 The PCPD also notes that the MRC scheme will adopt a proportionate approach and confine to specific categories of employees[1] of the banks whose conduct and integrity are more important and the need for addressing the RBA phenomenon is of relatively higher priority. The PCPD acknowledges that the information about an employee's conduct would be important to the recruiting banks in relation to the inherent nature of the job for which the employee is appointed.

Specific Comments

Collection of the specific information regarding the conduct of the prospective employee

9 The PCPD notes that under the MRC scheme, information regarding an employee's conduct will be collected by his/her employer throughout the employment and the records will be retained by the employer for 10 years.

10 While it is reasonable and legitimate for employers to maintain employment records and information an employee's conduct (such as written records of disciplinary proceedings) in the course of employment, Data Protection Principle (DPP) 1(3) requires data users (i.e. the employers) to take all practicable steps to ensure that employees are informed of certain matters in relation to the collection of their personal data, such as the purpose for which the data is to be used and the classes of persons to whom the data may be transferred.

11 Hence, upon implementation of the MRC Scheme, employers shall inform their employees that the type of data (including specific information regarding employees' conduct) that will be collected, how they will use the data and how they will transfer the data to prospective recruiting banks for reference checking. This notification requirement can be made in the form of a written Personal Information Collection Statement (PICS) pertaining to employment.

Accuracy and Duration of Retention of the employees' personal data

12 The proposed duration of MRC information would cover the prospective employee's employment records in the past 10 years up to the date of application for

[1] Phase 1 will cover directors and bank employees in senior management positions, while Phase 2 will extend the coverage to bank employees heading key supporting functions (including human resources, risk management, legal, compliance, internal audit and other equivalent units) and those who are having client facing or sales responsibilities (including staff carrying out securities, insurance and MPF-related regulated activities, as well as branch managers, tellers and customer relationship representatives).

employment. The PCPD notes that this proposal is in line with the HKMA's existing requirement that 10 years of employment records need to be disclosed by applicants in their applications to take up positions of directors, chief executives, alternative chief executives and executive officers.

13 For the purpose of the MRC scheme, all banks would have to maintain employment records of their employees who have ceased to be employed by the banks for a period of at least 10 years counting from the date of the employees' departure from the banks.

14 Pursuant to DPP2(2), all practicable steps must be taken to ensure that personal data shall not be retained longer than is necessary for the fulfillment of the purposes (including directly related purposes). Section 26 of the PDPO also requires that all practicable steps shall be taken to ensure erasure of personal data that is no longer required unless it is prohibited by law, or in the public interest not to do so. Contravention of section 26 of the PDPO is liable to criminal prosecution.

15 Generally speaking, an employer should implement a written data retention policy that specifies a retention period of no longer than seven years in respect of employment-related data held about an employee from the date the employee leaves employment unless there is a subsisting reason that obliges the employer to retain the data for a longer period or the former employee has given prescribed consent for the data to be retained beyond seven years[2]. As the MRC Scheme is for the legitimate purposes of tackling RBA issue and enhancing the integrity of the banking industry, the PCPD generally considers it as a subsisting reason and in the public interest for the employer to retain the data for a longer period.

16 Having said that, the PCPD considers that it would be fair if the employees are given a right to request for deletion of their data in specified circumstances, for example retirement and permanent departure from Hong Kong. Under these circumstances, it would no longer be necessary for the employers to retain the personal data of those employees.

17 Regarding the personal data of an unsuccessful job applicant, generally an employer should not retain the same for a period longer than two years from the date of rejecting the applicant unless there is a subsisting reason that obliges the employer to retain the data for a longer period or the applicant has given prescribed consent[3]. Hence, the recruiting banks, upon receiving the information from the reference providing banks, shall not keep the data for more than 2 years unless there are special circumstances warranting it to do so. These special circumstances, if any, shall be clearly documented.

---

[2] See paragraph 4.2.3 of the Code of Practice on Human Resource Management published by the Privacy Commissioner ("Code") at https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/PCPD_HR_Booklet_Eng_AW07_Web.pdf

[3] See paragraph 2.10 of the Code

18 The PCPD notes that all information provided under the proposed MRC Scheme should be supported by written documents, and to the best knowledge of the reference providing banks are being true, fair, complete, accurate and capable of substantiation. The PCPD agrees that accuracy and completeness of the employment records are imperative to the successful implementation of the MRC Scheme, not to mention that data accuracy is an essential element from the perspective of personal data privacy. In accordance with the requirements under DPP2(1)(a), an employer should take all practicable steps to maintain the accuracy of personal data retained for purposes that continue after the employee has left employment.

Consent by the Prospective Employee

19 In general, DPP3 provides that personal data shall not be used (including disclosed or transferred) by a data user (e.g. a frontline professional) for a new purpose without the express and voluntary consent of the data subject.

20 The PCPD notes that it is proposed that written consent should be obtained from the prospective employee to, *inter alia*, authorise the recruiting bank to conduct reference checking with his/her current and former employer banks and authorise the reference providing banks to disclose his/her employment records to the recruiting bank. The PCPD takes the view that obtaining an informed consent from the prospective employee is necessary, as this would ensure that the data subject consents to such disclosure and that the former employers could rely on the consent to proceed with the reference checking.

21 As the purpose of the MRC scheme is for the prospective employer to check the integrity of the prospective employee in a recruitment process, the prospective employer shall not use (including disclosure or transfer to any third parties) the employee's personal data for a new purpose. Noting that the proposed employee's consent only covers the prospective employer to conduct reference checking and the former employers to provide the records to the prospective employer, any further use of the employees' data for a purpose not directly related to these purposes would be considered as a new purpose and a fresh prescribed consent shall be obtained from the employee concerned.

An opportunity to be heard

22 It is noted that under the proposed MRC Scheme, the recruiting bank would provide the prospective employee with an opportunity to be heard in case there is any negative information from the reference providing banks. From the perspective of personal data privacy, this proposal would be in line with DPP6 and section 22 of the PDPO, which provides data subject a right to request correction of inaccurate personal data. As a matter of good practice, employers should implement measures and have policies and procedures in place to ensure that they can comply with a data correction request made by a job applicant, current or former employee.

Security of the personal data

23 The PCPD notes that under the proposed MRC Scheme, all banks should put in place adequate internal systems and controls, policies and procedures to safeguard integrity and confidentiality of information obtained and processed during the MRC process.

24 Pursuant to DPP4(1)(a), the kind of data and the harm that could result in case of unauthorized or accidental access are some of the factors to be considered when specifying the degree of security measures required. Hence, safeguards or security treatment should be commensurate with the sensitivity of the personal data. As the employment records and conduct of an employee are rather sensitive and may bring grave harm to a data subject if leaked, it is important to put in place adequate security measures to ensure that the data is securely kept and transmitted.

25 Adequate security measures shall be in place to prevent unauthorized access to any computer system, file(s) and/or cabinet(s) storing the employees' personal data. This would include, but not limited to, (1) proper access control defining who can access the data, such as multi-factor authentication before retrieving any data inside in the system and access to data by designated staff only for a legitimate purpose; (2) locking the cabinet(s) and (3) encrypting the data if needed to be transmitted and during storage.

Data Ethics

26 In addition to compliance with the requirements under the PDPO, data users shall also uphold the principles of accountability and data ethics when collecting and using personal data. It would therefore be important to observe the principles of explainability and transparency having regard to the rising expectations of the public. The ethical elements of data protection (namely being fair, respectful and beneficial) will bridge the gap between legal requirements and stakeholders' expectations.

Other matters

27 We take note of the consultation questions at Annex 1 of the Consultation Paper and understand that most of these questions are related to the operation and implementation of the MRC scheme. We are not in a position to offer any comments on the matters that are not related to personal data privacy as those matters are not within the purview of the PDPO.

The Privacy Commissioner for Personal Data, Hong Kong
August 2020