

# **Survey of Public Registers Maintained by Government and Public Bodies**

## **Executive Summary**

**Date issued: 28 July 2015**



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

## Executive Summary

### *Introduction*

1. Public registers contain personal data which can be made available for public access. They are subject to protection under the Personal Data (Privacy) Ordinance (the “**PDPO**”). In particular, the use of personal data collected from the public register is governed by Data Protection Principle 3. This is a use limitation principle which provides that personal data should only be used for the purposes for which it was collected or a directly related purpose, unless the explicit and voluntary consent of the data subject is obtained. In other words, the personal data collected from a public register can normally be used only for purposes in line with or directly related to the purpose of setting up the public register.

### *Data protection necessary to guard against privacy risks*

2. Personal data in the public registers, if used without regard to the original purpose of collecting the data and making it publicly available, or without appropriate safeguards, would attract a series of privacy risks, thus jeopardizing the interests of the data subjects.

3. For example, the unfettered access to information sources like the companies, land, and vehicles registers would put sensitive data such as Hong Kong identity card numbers, full residential addresses and signatures at stake. If the data was exploited by persons with malicious intent, the data subject would suffer the risks of financial loss, identity theft and personal safety (through stalking and surveillance).

4. In addition, there are risks of “function creep”, where data collected for one purpose is gradually used for other purposes such as direct marketing or data mining to which the individual has not consented. Further, information and communication technologies enable aggregation, matching and further processing of data in the public domain, thus creating profiles about people without their knowledge or consent. Such activities greatly increase their vulnerability to a variety of dangers, for example, human flesh search followed by cyber-bullying, and making decision and inferences about the individuals in ways that are unfair and discriminatory.

*The Government guidelines on safeguarding privacy and data protection for personal data in public registers*

5. Citizens have practically no choice when they surrender their personal data to the public registers maintained by the Government. It is therefore incumbent upon the Government to provide necessary legislative, administrative and technical safeguards to protect the data against indiscriminate use.

6. In this regard, the PCPD notes that in order to ensure that the administration of public registers by Government bureaux and departments complies with the requirements under the PDPO, the Home Affairs Bureau<sup>1</sup> issued a set of guidelines (the “**Guidelines**”) on 30 December 2000 on the protection of personal data in relation to existing and new public registers maintained / to be maintained by them.

*The Survey*

7. In order to ascertain the extent of compliance with the Guidelines by government public registers, the PCPD examined all the 82 ordinances (and related regulations) enacted or amended during the period from 1 January 2001 to 31 March 2014 which contain provisions relating to public registers. The PCPD also conducted a survey among 10 commonly-used public registers: Bankruptcy register, Births register, Business register, Companies register, Land registers, Marriage register, Register of notice of intended marriage, SFC register of licensed persons, Register of vehicles and Registers of electors.

8. The findings of the survey and the PCPD’s recommendations are summarized as follows.

9. Generally the registers are administered in accordance with the law, have Personal Information Collection Statement and statements of purpose to be acknowledged by searchers, but there is room for improvement.

---

<sup>1</sup> Since July 2007, the Constitutional and Mainland Affairs Bureau has taken over from the Home Affairs Bureau the policy area of personal data protection.

*Specify in legislation purpose of register and safeguards against misuse of data*

10. The Guidelines advise that the purposes of a public register should be stated as specifically as practicable in the legislation that establishes it.

11. The Guidelines also advise including provisions in the legislation to: (a) impose sanctions against the improper use of the personal data; (b) specify the purposes for which the data may be requested, and to limit the class of persons entitled to make requests; and (c) require requestors to declare in writing the intended use of the information requested.

*Findings*

12. Only 32 of the 82 ordinances (and related regulations) specifically spell out the purposes of the publication of the data and/or the permissible use or secondary use of such data. Only 5 of the 82 ordinances (and related regulations) contain explicit provisions introducing measures to safeguard against possible misuse of the personal data. The PCPD is not sure whether the apparent non-compliance represents an omission or the outcome of conscious decision.

*Recommendation*

13. The PCPD recommends the Government to establish a dedicated organisational structure and mechanism to oversee and monitor compliance with the Guidelines by the various Government bureaux and departments, particularly in regard to the required legislative enactment or amendment.

14. The PCPD envisages the Department of Justice, which occupies a gate-keeping position in the legislative process, could play a useful role in the monitoring process.

*Whether there are legitimate purposes to introduce the 10 public registers*

15. The disclosure of an individual's personal data to the public is itself an invasion of his privacy. Therefore, a public register should be introduced only where it would serve legitimate purposes.

### *Findings*

16. The purposes of the ten registers were gathered from the register operators. The PCPD has no reason to doubt that they serve legitimate purposes.

### ***Whether the purposes of the 10 public register are specified in the relevant legislations***

#### *Findings*

17. The purposes of the registers are specified in the respective legislations for only four registers.

18. For the remaining six registers, the respective legislations have been amended since the issue of the Guidelines in 2000 but the opportunities were not taken to incorporate provisions to specify the purposes of the registers. The PCPD has no knowledge as to why the opportunities were not taken to incorporate provisions. None of them has a timetable to introduce the required legislative provisions. Some of them even displayed complacency about the status quo.

#### *Recommendation*

19. The PCPD recommends to introduce a “personal data clearance clause” in the law drafting process, in line with the “human rights clearance clause” and the “basic law clearance clause”, and to assign the Department of Justice to take up the gate-keeper role to ensure that serious consideration will be given in future legislative enactment or amendment processes to incorporate the specific purposes of public registers.

### ***Whether safeguards against misuse of the personal data obtained from the 10 registers are included in the relevant legislations***

#### *Findings*

20. Compliance with the Guidelines has not been particularly enthusiastic. Only the Registers of electors have legislative safeguards and only the Register of vehicles provides for administrative safeguards.

21. There are no concrete timetables for introducing legislative safeguards in future. Some registers quoted the PDPO as the safeguard already in place. This is inappropriate as the Guidelines require an assessment of the sensitivity of the personal data in the respective registers and the potential adverse effect which any improper use would have on the data subjects, which may conclude that sanctions different from those provided under the PDPO are required.

22. The present state of affairs is unsatisfactory, particularly for those registers where the register operators seemingly have no discretion to reject a request for inspection (see paragraph 30 below), and data protection is therefore dependent wholly on safeguards against misuse.

### *Recommendation*

23. The proposed dedicated body responsible for overseeing and monitoring compliance with the Guidelines should ensure that bureaux and departments do capitalize on any future legislative process to consider incorporating provisions to safeguard against misuse of personal data in public registers. Meanwhile, it should consider drawing up a timetable for the registers to formulate administrative safeguards as an interim measure.

### ***Whether data subjects are informed of the specified purposes of the 10 registers***

24. The Guidelines advise that the data subjects should be informed of the purposes of the registers and that their personal data is disclosed to the public.

### *Findings*

25. Data subjects are so informed by all 10 registers but the clarity and adequacy of the notification could be improved. The emphasis of the message is more on why the registers require the personal data and less on why the data needs to be disclosed to third parties. In three cases, namely, the Bankruptcy register, the Business register and the Marriage registers, there is no specific mentioning at all that the data can be made available to the public.

26. In the case of the Marriage register, the data subjects are requested to provide additional personal data for the purpose of compiling statistics and research purposes, but they are not explicitly informed in writing that provision of the additional data is voluntary.

### *Recommendation*

27. Where appropriate, the registers should explain more clearly to the data subjects why their personal data needs to be made available to the public.

28. Marriage register should inform data subjects in writing that provision of additional personal data for statistics and research purposes is voluntary.

### ***Whether only personal data necessary to fulfil the specific purposes of the 10 registers is collected***

29. According to the Guidelines, the data to be collected and disclosed in the public register should be specified in the relevant legislation. The types of personal data specified should be no more than necessary to fulfil the specified purpose of the register.

### *Findings*

30. The establishing legislations of eight registers contain provisions imposing a duty upon the relevant operator to provide specific kinds of personal data upon a search request and payment of fee. It seems that the operator has no control but to comply with each and every request.

31. For the remaining two registers (Marriage register and Registers of electors), the operators have definite discretionary power to decide on the provision of specific kinds of personal data or the full copy of the relevant document upon request. However, there are no explicit policies laid down governing the exercise of the discretion.

32. There are instances where personal data specified in the statutory form is no longer required. For example, the Registrar of Marriages has taken the discretion to allow the marrying parties to state on the Notice of Intended Marriage only the street name and district (instead of inputting the full address), and to omit input to the column for “occupation”.

### *Recommendation*

33. The legislations governing the types of personal data to be collected and publicly disclosed should be updated to reflect the actual need.

34. Where operators of the registers have discretionary powers to disclose the requested data, they should devise policies and practices to ensure that the personal data disclosed in compliance with a request is not more than necessary for the purpose of the registers.

35. When providing personal data of a sensitive nature (such as identification documents and residential addresses), operators of registers should explore less privacy-intrusive means of public disclosure of the data, for example, the provision of partial (instead of full) identification document number and the provision of correspondence address or incomplete address (instead of full residential address).

36. It is opportune for the Government to resurrect its earlier proposals to limit the disclosure of identification numbers and residential addresses of company directors filed with the Companies Registry.

***Whether persons accessing the 10 registers are advised not to use the personal data therein for any purpose unrelated to the specified purposes***

37. The Guidelines advise that all persons accessing or requesting access to a public register should be made aware of the specified purposes of the register and the need to confine the subsequent usage of the data collected from the register to such purposes.

*Findings*

38. The Guidelines are observed except the Register of notice of intended marriage. In the case of the Register of notice of intended marriage, no reference is made to the purpose of inspection of the notices throughout the process of inspection which takes place in the Marriages Registries by reviewing the webpages of onsite computers.

39. For online access to a public register, the Guidelines only require the home page to include the specified purposes of the register and the use limitations. To ensure the requestor does read and understand this homepage message, the registers, with the exception of the SFC register of licensees, require the requestor to acknowledge the message before access is allowed.



40. Other best practices adopted by the registers include requiring the requestor to (i) acknowledge the notification as regards the purpose of the register, the use limitations and the adverse consequences of misuse of requested information; and (ii) to declare the intended use of the requested information.

#### *Recommendation*

41. The Register of notice of intended marriage should devise measures to draw the attention of the person accessing the register to the purpose of inspection of the notices and the use limitations.

42. The best practices adopted by some registers should be followed by others, where appropriate. These include requiring the requestor to (i) acknowledge the notification as regards the purpose of the register, the use limitations and the adverse consequences of misuse of requested information; and (ii) to declare the intended use of the requested information.

43. In particular, for the SFC register of licensees, online requestors should be required to indicate that they have read the notification before proceeding with the search.

#### ***Whether search keys are limited to those required to fulfil the specified purposes***

44. The Guidelines advise that search keys should not be more powerful than is required for the specified purposes of the public registers. Where online access or electronic copies are available, steps shall be taken to prevent the re-configuration of the data which, in conjunction with a new search key, may enable the use of the data in a privacy intrusive manner.

#### *Findings*

45. The registers offering online searches have set some search key limits in facilitating online access.

46. The three registers which arrange bulk supply of register information all have service terms and conditions which prohibit against the misuse of requested data, including the manipulation or re-configuration of the data. Two of them also possess technical safeguards against data re-configuration.

***Whether bulk disclosure of public register information is allowed only where this is compatible with the purpose for which the information therein is made available***

47. The Guidelines advise against the bulk disclosure of personal data held by a public register unless there are strong reasons supporting such disclosure.

*Findings*

48. All the three registers which arrange bulk supply of register information have legitimate grounds supporting bulk disclosure.