Financial Services and the Treasury Bureau
Financial Services Branch
Personal Data Privacy Policy

This document sets out the Personal Data Privacy Policy of the Financial Services Branch ("FSB").

The Policy

2. FSB is committed to ensuring that all personal data are handled in accordance with the provisions of Personal Data (Privacy) Ordinance ("PD(P)O") including the Data Protection Principles and code of practices issued by the Privacy Commissioner for Personal Data ("Privacy Commissioner").

Personal Data

3. "Personal Data" as defined in the PD(P)O means any data -

(i) relating directly or indirectly to a living individual;
(ii) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
(iii) in a form in which access to or processing of the data is practicable.

Examples of personal data include an individual's name, address, Hong Kong Identity Card number, mobile phone number, education qualification, employment history and health records.

Data Protection Principles

4. PD(P)O requires data users to follow the fair information practices incorporated in the six Data Protection Principles. Under these principles data subjects have certain rights, including the right to be informed of whether a data user holds their personal data, to be supplied with a copy of such data and to request correction of any data they consider to be inaccurate. Non-compliance with a data protection principle may lead to a complaint to the Privacy Commissioner. A claim for compensation may also be made by a data subject who suffers damage by reason of a contravention of a requirement under PD(P)O. All officers who have responsibility for handling personal data should

familiarize themselves with the six Data Protection Principles set out in Schedule 1 of PD(P)O. The six Data Protection Principles are at **Appendix 1**.

Implementation of the Policy

5. FSB will implement its Personal Data Privacy Policy through the measures/arrangements set out in ensuing paragraphs.

(a) Collection of personal data

6. When collecting personal data, the following conditions should be satisfied –

(i) the purposes for which the data is collected are lawful and directly related to a function or activity of FSB;

(ii) the means of collection are lawful and fair in the circumstances of the case;

(iii) the personal data collected is necessary and adequate, but not excessive, for the purpose(s) for which it is collected;

(iv) the data subject is informed of whether it is obligatory or voluntary for him/her to supply the data and, if obligatory, the consequences of not doing so; and

(v) the data subject is informed of the purpose for which the data is to be used, the classes of persons to whom the data may be transferred, the rights of the data subject to request access to and correction of the data, and the name and address of the individual to whom any such request may be made.

7. To comply with the above notification requirements, a Personal Information Collection Statement ("PICS") (at **Appendix 2)** may be used when collecting personal data from individuals. The individuals could be provided with the PICS on or before the collection in an appropriate format and manner (e.g. in the same paper form or web page that collects the personal data).

(b) Accuracy and retention of personal data

8. A personal data inventory containing the following information is maintained by FSB –

(i) the kinds of personal data that FSB holds;
(ii) the purposes for which the personal data is collected, used and disclosed; and
(iii) how the personal data is stored.

We would also examine whether there is a continued need to hold such personal data, whether the use (including transfer and disclosure) of the data is in compliance with the provisions in PD(P)O, and whether the inventory is accurate and up-to-date on an annual basis.

9. Personal data will not be kept longer than is necessary for the fulfillment of the purpose (including any directly-related purpose) for which the data is or is to be used. File disposal exercises on records containing personal data will be conducted in accordance with the government records management guidelines and procedures. Destruction of paper records must be carried out by irreversible means and electronic records must be cleared or destroyed from storage media before disposal by means of sanitisation or physical destruction. Should there be a need to retain the personal data for statistical purposes, such data should be permanently anonymised so that the individuals concerned could no longer be identified.

(c) Use of personal data including the requirement of consent

10. All personal data collected should be used (including disclosure and transfer) only for the purposes of collection.

11. If personal data is used for a purpose other than the purposes of collection, the express consent of the data subject in writing for the use of the data must be sought beforehand. In seeking the data subject's consent, it must be made clearly understandable and readable that he/she is entitled to withhold his/her consent or withdraw his/her consent subsequently by giving notice in writing.

(d) Security of personal data

12. The following security arrangements are in place and will be reviewed regularly to ensure that personal data is properly protected and handled –

(i) personal data is classified as "Restricted" information which should be stored in a locked steel filing cabinet or in an office which is locked up after office hours and to which members of the public do not have access. Transmission and carriage of "Restricted" information is also bound by relevant regulations. Spot check would be conducted periodically to ensure compliance with relevant regulations;

(ii) restriction of the access to personal data on a "need-to-know" basis;

(iii) review and make improvements as appropriate of security measures for protection of personal data in the servers, user computers, transmission of electronic messages, etc.;

(iv) regular reminders to all staff to remind them to erase personal data in emails and other documents in their computers which are no longer required, and to avoid improper disclosure of personal data in letters and other communications;

(v) regular change of passwords for IT facilities, accounting and personnel systems, etc.;

(vi) encryption of all backup tapes that are to be transported to offsite storage;

(vii) review of office security such as access rights to individual zones within the office; and

(viii) personal data should not be provided on phone enquiries given the difficulty in ascertaining one's identity over the

phone; and

(ix) taking or copying of office documents containing personal data for use at home is prohibited unless prior approval is obtained from the relevant authority as follows –

(a) DS(FS)es – to be approved by PSFS personally;

(b) Team heads – to be approved by subject DS(FS)es; and

(c) Other officers of teams – to be approved by team heads.

(x) personal data must be encrypted when stored on mobile devices or removable media issued to individual officer. Officers securing approval for taking personal data outside office premises may contact EO(FS)1 for an encrypted USB device for storage of such data.

(e) Transparency of the Personal Data Privacy Policy and Practices

13. The Statement of FSB's Personal Data Privacy Policy and Practices including the kind of personal data currently held by FSB and the main purpose of using such personal data can be found in **Appendix 3**. This statement will be made available at our reception counter and be uploaded to FSB's website so that members of public are made aware of the procedures to access and correct their personal data held by FSB in accordance with Data Protection Principle 6.

(f) Requests for Data Access / Correction under the Ordinance

14. Internal procedures for handling requests for Data Access / Correction under PD(P)O including refusal of requests are set out at **Appendix 4**.

Timeframe

15. All requests made under PD(P)O must be dealt with as soon as practicable but, in any case, not later than 40 calendar days after receiving the request. The General Registry will alert the appropriate officers 2 weeks before the due date.

Charges

16. Unless approved otherwise, a charge will be made to cover the cost of photocopying personal data at the standard rate prescribed by the Director of Accounting Services. At present, the rate is $1.50 or $1.60 (w.e.f. 24.11.2023) per photocopy on documents provided in black and white on A4 or A3 size paper respectively with or without enlarging. Photocopying made on both sides of a sheet is counted as two copies. We are entitled to refuse to comply with a data access/correction request unless and until the fee has been paid.

Appeal

17. Refusal of requests for access to or correction of personal data must be endorsed by a Directorate Officer. A data subject may lodge an appeal against an earlier decision to reject a data access or correction request. The subject Directorate Officer would be invited to review his earlier decision and put up recommendation to the respective DS(FS) for a decision.

Incident Reporting and Breach Handling

18. A mechanism is set up at **Appendix 5** for incident reporting and breach handling in case there is loss or leak of personal data in FSB.

Ongoing Monitoring and Review

19. FSB maintains the following to ensure compliance with the Ordinance –

(i) the Statement of Personal Data Privacy Policy and Practices in accordance with Data Protection Principle 5 (**Appendix 3**);

(ii) a Central Register (template at **Appendix 6**) on requests for

access to or correction of personal data made to FSB; and

(iii) a Log Book for Registering **Refusal** of Requests for Access/Correction of Personal Data (template at **Appendix 7**) as required under Section 27 of PD(P)O.

20. The Personal Data Privacy Policy of FSB will be reviewed regularly and given to all newly joined officers with other induction materials. Officers handling personal data would be arranged to attend relevant training courses to keep themselves updated of the latest personal data policies as and when necessary.

Risk Assessment

21. Periodic risk assessments would be conducted to ensure that the policies, procedures and practices of personal data protection remain robust, and to identify potential areas where there may be breaches. Risk assessments should be conducted for all new projects involving personal data and on any new collection, use or disclosure of personal data in ways that are materially different from existing practice. Results of risk assessments conducted would be properly documented.

Circulation

22. This policy would be recirculated every 6 months.

Enquiries

23. All enquiries about this circular should be addressed to CEO(FS) at 3655 5105, or SEO(FS) at 3655 5155.

Financial Services Branch
Financial Services and the Treasury Bureau
December 2014