(Updated on 23.11.2017)

Appendix I

Privacy Management Programme of HA/HD
Policies and Practices

Organisational commitment

Governance Structure

HA/HD is committed to launching a PMP as part of our corporate responsibilities. To this end, Assistant Director (Administration) ("AD(Adm)") is designated as the officer-in-charge with overall responsibility in overseeing the implementation of the PMP and compliance with the PDPO.

2. AD(Adm) is supported by Chief Executive Officer (Human Resource Management)1 who, along with Senior Executive Officer/Personnel (1) (who has been designated as the Departmental Data Protection Officer ("DDPO")), oversees the day-to-day compliance matters.

3. The DDPO would, in collaboration with the following Divisional DPOs ("DivDPOs"), co-ordinate action in response to data access/correction requests made under the PDPO and other personal data privacy-related issues such as complaints and breaches.

Division	DivDPO	Designation
Development and Construction Division	Chief Quantity Surveyor 1	DivDPO(DCD)
Estate Management Division	Housing Manager (Management)	DivDPO(EMD)
Permanent Secretary's Office, Corporate Services Division and Strategy Division	Senior Publicity Manager (Complaints and Enquiries)	DivDPO(CSD, SD, SRPA & PSH Office)

Reporting

4. The procedures for handling complaints received on referral from PCPD are set out in paras. 14 to 18 below. Insofar as management reporting is concerned,

DDPO would report the statistics, trend and follow-up progress in respect of privacy-related complaints to the Senior Official Meeting ("SOM") on a monthly basis in the SOM paper on Complaint Statistics co-ordinated by the Complaints and Enquiries Sub-section.

5. Data breach cases should be reported as soon as practicable to the DivDPO concerned who should, in consultation with DDPO, propose to AD(Adm) on how the case should be handled, including whether it should be brought to the attention of the senior management, the PCPD and/or other parties. The procedures to follow in handling data breach cases are set out in paras. 19 and 20 below.

Programme Control

Personal Data Inventory

6. Understanding and documenting the types of personal data that HA/HD collects and where it is held (e.g. whether or not the data has been passed to any data processor – see paras. 21 to 23 below) are important. This will affect the type of consent we obtain from individuals and how the data is protected. It will also make it easier to assist individuals in exercising their data access and correction rights.

7. Broadly, personal data kept by HA/HD can be classified under the following categories –

(i) Staff employment-related personal data
(ii) Customer data
(iii) Business associate data
(iv) HA-related personal data

8. A personal data inventory setting out details of the above data, including the purpose of collection, usage, location, retention period, contact persons for public enquiries, etc. is at **Annex 1**.

9. All sections should maintain its own personal data inventory and keep it up-to-date, ready for inspection by prospective data subjects upon request. By close of January every year, sections should submit an updated inventory to the DivDPO concerned showing the position as at 31 December of the previous year. On the basis of these sectional inventories, DivDPOs should compile the inventory for their respective divisions/units, and accordingly, DDPO will compile HA/HD's inventory in the form of Annex 1. The inventory will be made available for inspection if necessary.

Policies addressing obligations under the PDPO

10. HA/HD has established policies to address obligations under the PDPO, including those in the following areas –

(i) Collection of personal data
(ii) Accuracy and retention of personal data
(iii) Use of personal data including requirements for consent
(iv) Security of personal data
(v) Transparency of personal data policies and practices
(vi) Access to and correction of personal data

Details of these policies are set out at **Appendix II** to DGC No. 1/2015. Staff should observe these policies in every function of their operations involving use of personal data.

Risk Assessment

11. Privacy risk assessment in HA/HD should be conducted on the following two dimensions –

(i) identifying and mitigating leakage and security risks in respect of personal data currently in possession; and

(ii) vetting new policies, projects and practices involving personal data, as well as new collection, use or disclosure of personal data in ways that are materially different from existing practice with a view to minimizing personal data impact.

12. The procedures to follow in conducting privacy risk assessment are set out in Part III of **Annex 2**.

Staff training and education

13. As a matter of established practice, HA/HD provides newly appointed staff members with personal data protection training in induction programmes and periodically thereafter. Regular staff training covering general policies/procedures and topical data protection issues would also be arranged in collaboration with PCPD.

Complaint handling

14. Failure on the part of the Department or individual office/staff member to comply with the requirement of the PDPO may be the subject of public complaints.

HA/HD is committed to responding to personal data privacy-related complaints promptly, rectifying inadequate and/or irregular practices revealed thoroughly, and through regular reviews (as noted in para. 4 above), refining operational practices and preclude recurrence.

15. Complaints originating from staff should be processed in accordance with Departmental Staff Circular No. 3/2009 on "Staff Complaints Procedures" (replaced by Departmental Staff Circular No. 6/2016 on 21.12.2016). Complaints originating from the PCPD should be processed as per para. 16 below. Complaints originating from other sources should be processed in accordance with Departmental General Circulars No. 1/2012 on "Procedures in Handling Public Complaints" (replaced by Departmental General Circular No. 5/2015 on 26.6.2015) and No. 3/2008 on "Procedures for Handling Ombudsman Cases".

16. Complaints originating (including those on referral) from the PCPD should be forwarded to the subject office for follow up action and copied to the relevant DivDPO. The subject office should duly investigate any complaint received and clear its findings/recommendations with an officer at D1 rank or above before responding to the complainant/originator (including PCPD). The reply should be copied to the DivDPO concerned. If a complaint involves serious data breach (e.g. loss of a large number of sensitive personal data) or carries potential sensitivities (e.g. media interest), the DivDPO should, in consultation with DDPO, bring it to the attention of AD(Adm) and the DD concerned. If legal or general compliance issues arise or if the complaint involves claims against the department, the subject office should consult Legal Services Sub-division ("LSSD") where appropriate.

17. The position of complaints received on referral from PCPD should be reported on a monthly basis in the Senior Official Meeting paper on Complaint Statistics. To facilitate timely reporting, subject offices should keep DDPO and the DivDPO concerned abreast of the development of all outstanding cases.

18. Complaints may reveal inadequacies or irregularities in operational practices. As part of the follow-up actions on a complaint case, the DivDPO and Division concerned should review their practices and take remedial or refinement measures where appropriate.

Breach handling

19. A data breach is generally taken to be a suspected breach of data security of personal data held by a data user, exposing these data to the risk of loss, unauthorised or accidental access, processing, erasure or use. In handling a case of data breach, the investigating officer should refer to the following guidelines –

(i) Guidance note on "Data Breach Handling and the Giving of Breach Notifications" published by the PCPD at http://www.pcpd.org.hk under ~~"publications and videos"~~ *"Resources Centre / Publications / Guidance Note"*;

(ii) Chapter VIII of Security Regulations; and

(iii) "Information Security Incident Response Procedure" of HA/HD at e-housing under IT security.

20. Data breach, once identified, should be reported to the relevant DivDPO. If the case is serious (e.g. involves loss of sensitive personal data) or carries potential sensitivities (e.g. media interest), the DivDPO concerned should report to DDPO, AD(Adm) and the DD concerned. If it is considered that the case should be reported to the PCPD, PS(H)'s agreement should be sought and Head (Information & Community Relations) should be informed before reporting.

Data processor management

21. A data processor is a person who –

(i) processes personal data on behalf of another person; and

(ii) does not process the data for any of the person's own purposes.

Some examples of data processor engagement in the HA/HD context are as follow –

(i) Day-to-day management of public rental housing estates is outsourced to commercial Property Services Agents ("PSAs"). PSAs are required to check the personal data such as copies of identity cards, marriage certificates or salary documents etc. from Public Rental Housing residents for verification of applications. These documents will be submitted to HD staff for processing as required under different tenancy policies.

(ii) Labour Relations Officers ("LRO") are provided to individual site of capital works new works contracts by service providers engaged by HA. The main duty of the LROs is to assist project teams to check documents, including copies of workers' employment contracts, attendance records, wage payment and MPF contribution records for implementation of the Wage Monitoring System with a view to safeguarding wage payment to workers in accordance with the relevant regulations and avoiding wage disputes.

22. If a data processor is engaged (within or outside Hong Kong) to process personal data on behalf of HA/HD, the office concerned must adopt contractual or other means to –

(i) prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data; and

(ii) prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

23. Staff may refer to the PCPD publication entitled "*Outsourcing the Processing of Personal Data to Data Processors*", which may be downloaded at http://www.pcpd.org.hk under *"Resources Centre / Publications / Information Leaflets / Others"* ~~*"publications and videos"*~~, for guidance. In formulating contractual agreement with data processors, advice of the LSSD should be sought where necessary.

Communication

24. Openness about HA/HD's privacy policies, practices and compliance measures is part of our corporate accountability. In this connection, HA/HD has devised its Privacy Policy Statement. The Statement contains the following information –

(i) HA/HD's commitment to ensuring that all personal data are handled in accordance with the provision of the PDPO;

(ii) a general description of the types of personal data being held by HA/HD the types of personal data that may be collected when members of the public visit our website, the purpose(s) of collecting such data, and the way requests for accessing and correcting such data may be made, etc.;

(iii) the contact details of the DDPO to whom data access/correction requests may be addressed;

(iv) the charges for supplying copy of personal data; and

(v) other practices of HA/HD in complying with the Ordinance, such as maintaining a Central Register of data access/correction requests and formulating departmental guidelines on compliance, etc..

The Statement is published on HA/HD's website at http://www.housingauthority.gov.hk/. A hard copy is displayed in the public reading

area of the Housing Authority Library on 4/F, Block 3 of the Housing Authority Headquarters Building.

Ongoing assessment and revision

25. Through the following measures, we seek to monitor, assess and where appropriate, refine our privacy management framework to ensure that it remains relevant and effective –

(i) monthly report to SOM to keep senior management abreast of latest complaint situation and trend, and areas to note/follow up on compliance (para. 4 above);

(ii) annual review of Personal Data Inventory to ensure that it provides up-to-date information on personal data in our possession; data disposal be done timely for personal data in respect of which the purpose of collection no longer applies; and measures in respect of data processors be taken, etc. (paras. 6 to 9 above);

(iii) review on security arrangements once every two years to ensure that personal data is protected from unauthorised use or accidental leakage;

(iv) risk assessment once every two years (paras. 11 and 12 above);

(v) review on training performance (classes held, attendance, coverage, projected requirement, new areas of attention, etc.) once every two years; and

(vi) reports on the implementation of PMP to be submitted to AD(Adm) once every two years covering (ii) to (v) above and other issues, e.g. breach and incident management response review, etc.

26. DivDPOs should use the proforma at Annex 2 to complete item (ii) above once every year and items (iii) and (iv) above once every two years in collaboration with offices in their respective division/units before 31 January. On this basis, DDPO will report the updated personal data inventory, privacy risks identified/contemplated and training performance to AD(Adm) once every two years along with an analysis of the present state of compliance and a projection of foreseeable privacy issues arising from, say, new policies/practices.