港燈電力投資
HK Electric Investments

Personal Data Privacy Policy

September 2020

Table of Contents

1. Introduction

1.1 HK Electric Investments Limited and its subsidiaries including The Hongkong Electric Company, Limited (collectively, the "**Group**") is committed to respecting and safeguarding the privacy of individuals' personal data. We need to ensure that we comply with the Personal Data (Privacy) Ordinance Cap 486 including any statutory modification or reenactment thereof, supplements, revisions and amendments in force from time to time and any subsidiary legislation (the "**Ordinance**") and the relevant codes of practice which may be issued and updated by the Office of the Privacy Commissioner for Personal Data ("**PCPD**") from time to time.

1.2 This Policy sets out the structured framework for the Group to follow in protecting personal data privacy. It applies to all directors and employees of the Group who shall also observe any additional personal data policies, rules, regulations, requirements and guidelines to which they may be subject from time to time.

1.3 It is a joint effort by all to ensure that the relevant laws on personal data privacy are complied with and that effective measures are adopted to protect personal data concerning a wide spectrum of data subjects such as our customers, guests, contractors, unit holders, visitors, job applicants, employees and other stakeholders and persons involved in our businesses. Violation of the Ordinance may result in civil or criminal sanctions, as well as serious harm to the Group's reputation.

1.4 Non-compliance with this Policy, including non-compliance with any guidelines issued pursuant to this Policy, may give rise to disciplinary action including summary dismissal.

2. Personal Data

2.1 Personal data means any data relating directly or indirectly to a living individual (which is referred to as the "**data subject**"), from which it is practicable to ascertain, directly or indirectly, the identity of the individual, and which are in a form in which access or processing is practicable.

2.2 Personal data must be collected, used, disclosed and retained in a manner observing the six data protection principles (each a "**DPP**") which are set out in Schedule 1 of the Ordinance. The six DPPs represent the normative core of the Ordinance and cover the life cycle of a piece of personal data.

3. Identification of Personal Data

The Group has to identify the personal data in its custody and control. Each business unit ("**BU**") should maintain an inventory of the kind of personal data it collects and/or uses.

4. Collection of Personal Data
(DPP1 – Data Collection Principle)

4.1 Personal data collected by the Group shall be for a lawful purpose and by lawful and fair means, and directly related to a function or activity of the Group. The data collected should be necessary but not excessive in relation to that purpose.

4.2 When personal data are collected from a data subject, all practical steps should be taken to notify the data subjects on or before collection of the data:

4.2.1 the purpose for which the data are to be used;
4.2.2 the classes of persons to whom the data may be transferred;
4.2.3 whether the supply of data is obligatory or voluntary;
4.2.4 the consequences of failing to supply the data; and
4.2.5 the data subject's right to access and correct the data

The best practice to fulfill these requirements is to provide data subjects with a Personal Information Collection Statement ("**PICS**").

5. Accuracy and Duration of Retention of Personal Data
(DPP2 – Data Accuracy and Retention Principle)

5.1 The Group should ensure that the data held are accurate and up-to-date. If there is doubt as to the accuracy of the data, use of the data should stop immediately.

5.2 The Group should not keep the data any longer than is necessary for the purpose for which the data were collected, i.e. personal data should be disposed of when it is no longer required for the purpose for which it was originally collected.

6. Use of Personal Data
(DPP3 – Data Use Principle)

6.1 Unless with the express prior consent given voluntarily by the data subject or otherwise permitted by law, the Group should not use the personal data for any purpose other than the one mentioned at the time the data were collected or a directly related purpose.

6.2 In seeking the data subject's consent required for a new use of the personal data collected, all practical steps should be taken to ensure that (i) information provided by the data subject is clearly understandable and readable; and (ii) the data subject is informed that he or she is entitled to withhold or withdraw his or her consent subsequently by giving notice in writing, and where applicable, the consequences of doing so.

6.3 The Group may disclose personal data for any purpose in respect of which an exemption is available under the Ordinance or pursuant to a mandatory legal requirement.

6.4 Data subjects should be informed (for instance, through the PICS) of the possible transferees of their personal data when their personal data is collected.

7. Security of Personal Data

(DPP4 – Data Security Principle)

The Group should take appropriate security measures to protect personal data, and should ensure that personal data are adequately safeguarded against unauthorised or accidental access, processing, erasure, loss or use.

8. Information to be Generally Available

(DPP5 – Openness Principle)

The Group should take all reasonably practical steps to make known to the public its personal data policies and practices, the kinds (but not the content) of personal data it holds and the purpose for which the data is or is to be used.

9. Personal Data Access and Correction

(DPP6 – Data Access and Correction Principle)

9.1 The Group should recognise and respond to a data subject's right to request access to personal information, including whether or not it holds any of his/her personal data, and to request a copy of such personal data held by that user.

9.2 If it is found that the data contained therein is inaccurate, the data subject has the right to request the data user to correct the record.

9.3 The Group should accede to the access and correction requests made by the data subject as soon as practicable but in any event not later than 40 days after receiving the request under normal circumstances.

10. Data Processors and Third Party Service Providers

10.1 Where data processors and third party service providers are engaged to provide services which will require them to process, or may allow them to come into contact with personal data, a confidentiality agreement or a service contract incorporating certain terms regarding personal data protection must be in place before they are allowed to commence their services to ensure that the data will be kept confidential and will not be kept longer than is necessary. For more details, please refer to "Guidelines for Data Processor Management" issued by the DPO (as defined in paragraph 12.3 below).

10.2 Each BU should maintain a register of data processors and third party service providers having access to the personal data under the BU's control and custody, and identify agreement referred to in paragraph 10.1 entered into by the data processors and third party service providers.

11. Direct Marketing

11.1 Direct marketing activities include the offering or advertising of the availability of goods, facilities or services and the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political and other purposes.

11.2 The Group should not use personal data for any direct marketing activities without first complying with the Ordinance including the following requirements:

11.2.1 giving the individuals (from whom the personal data is collected) an informed choice of deciding whether or not to allow the use of their personal data in direct marketing;

11.2.2 must not use or provide personal data to others for use in direct marketing without data subject's consent or indication of no objection; and

11.2.3 are requested to honour and update the data subject's request for ceasing the use of his/her personal data.

For further explanation of these requirements, please refer to "The New Guidance on Direct Marketing" published by the PCPD.

11.3 The Heads of the BUs (the "**BU Heads**") are responsible for assessing whether any of its business activities constitutes a direct marketing activity.

11.4 Each BU should indicate clearly on its personal data inventory whether the relevant personal data may be used for the direct marketing activities it undertakes from time to time.

11.5 Employees having responsibilities for direct marketing are required to have sufficient knowledge with the applicable personal data privacy requirements. They should read "The New Guidance on Direct Marketing" and any other relevant guidelines/guidance published by the PCPD from time to time.

12. Privacy Management Programme

12.1 Privacy Management Programme ("**PMP**") is a strategic framework to assist building robust privacy infrastructure supported by effective on-going review and monitoring process, and facilitate compliance with the requirements under the Ordinance. The Group's PMP demonstrates its organisational commitment to have an internal governance structure in place that fosters a culture of respectful privacy, and provides for the programme controls required for an effective governance structure.

12.2 The Group assigns the following personnel to assist in the implementation and management of the PMP, and their roles and authorities are as follows:

Personal Data Protection Officer

12.3 The Group Legal Counsel and Company Secretary is the Personal Data Protection Officer (the "**DPO**"), responsible for managing the implementation of the PMP and facilitating the Group's compliance of the Ordinance.

12.4 The DPO is responsible for:

12.4.1 establishing and implementing the PMP programme controls on the Group's personal data inventory, including without limitation issuing guidelines on personal data inventory, periodic risk assessment, privacy impact assessments, training and education, handling of data breach incidents, data processor management and personal data information collection statement … etc., and for such purposes, issue guidelines for these PMP programme controls;

12.4.2 reviewing the effectiveness of the PMP and revising the programme controls where necessary, including preparing oversight and review plan and conducting annual review of the effectiveness of the PMP; and

12.4.3 representing the Group in the event of an enquiry, inspection or investigation on significant personal data incidents by the PCPD and and/or other law enforcement agencies.

BU Heads

12.5 BU Heads have the primary responsibility to ensure their BUs' compliance with the Ordinance and this Policy, identify the inventory of personal data collected by their BUs, develop and implement appropriate data protection measures, and assess and monitor the effectiveness of the control and other measures put in place to comply with the Ordinance and the PMP and give effect to this Policy.

12.6 When devising personal data protection measures, BU Heads should draw reference to the relevant guidelines published by the PCPD, where available and applicable, from time to time. The recommendations in the guidelines should, where applicable, be incorporated into their BUs' policies and practice.

Customer Personal Data Protection Officer

12.7 The Head of Customer Supplies, Customer Services Division is the Customer Personal Data Protection Officer.

12.8 The roles and authorities of the Customer Personal Data Protection Officer are:

12.8.1 establishing and implementing PMP programme controls specific to personal data for the Group's electricity customers ("**customer personal data**") and for such purposes, issue guidelines for these PMP programme controls;

12.8.2 handling privacy complaints or enquiries in relation to customer personal data or PMP for such data;

12.8.3 handling data access or correction requests under the Ordinance in relation to customer personal data;

12.8.4 handling of an enquiry, inspection or investigation by law enforcement agencies for customer personal data; and

12.8.5 liaising with the DPO as necessary in connection with the above matters.

Employee Personal Data Protection Officer

12.9 The Senior Manager (Compensation & Benefits Division), Human Resources Division is the Employee Personal Data Protection Officer.

12.10 The roles and authorities of the Employee Personal Data Protection Officer are:

12.10.1 establishing and implementing PMP programme controls specific to personal data for the Group's employees (which shall include personal data for prospective or past employees or otherwise obtained for any purpose which relates to their employment with the Group)("**employee personal data**") and for such purposes, issue guidelines for these PMP programme controls;

12.10.2 handling privacy complaints or enquiries in relation to employee personal data or PMP for such data;

12.10.3 handling data access or correction requests under the Ordinance in relation to employees personal data;

12.10.4 handling of an enquiry, inspection or investigation by law enforcement agencies for employee personal data; and

12.10.5 liaising with the DPO as necessary in connection with the above matters.

BU Personal Data Coordinator

12.11 Each BU should appoint a coordinator (the "**BU Personal Data Coordinator**") to liaise and communicate, as the BU's representative, with the DPO, the Customer Personal Data Protection Officer and the Employee Personal Data Protection Officer, as applicable, regarding the status of compliance of the Ordinance and this Policy and matters related to the PMP, and to support the BU Heads in the discharge of their responsibilities. A BU Head can act as the BU Personal Data Coordinator, if considered to be appropriate.

12.12 The BU Personal Data Coordinators' roles include:

12.12.1 conducting the annual review of the personal data inventory of their respective BUs and submitting the updated inventory to the DPO through uploading onto the corporate portal;

12.12.2 carrying out periodic risk assessments within their respective BUs by completing the risk assessment questionnaire issued by the DPO, and submitting the completed questionnaire through uploading onto the corporate portal;

12.12.3 conducting data processors management review for their respective BUs by completing the data processors management review checklist issued by the DPO, and submitting the completed checklist to the DPO through uploading onto the corporate portal;

12.12.4 arranging the disposal of record containing personal data in accordance with the relevant records management guidelines and procedures;

12.12.5 arranging general training on personal data protection for their respective BUs to ensure compliance of the Ordinance and, where appropriate, seek assistance from the DPO to arrange training on specific topics; and

12.12.6 assisting the DPO in carrying out the ongoing assessment and revision of the PMP.

13. Breach Handling and Reporting

13.1 Employees should be alert and vigilant with respect to any violation or suspected violation of personal data protection. Any breach or suspected breach of security of personal data held by the Group or this Policy should be immediately reported in accordance with the "Guidelines for Data Breach Handling" issued by the DPO.

13.2 Any breach or suspected breach of this Policy (including any guidelines issued pursuant to this Policy) can be reported to the BU Head, the DPO, the Head of Internal Audit or the Group's whistleblower hotline. The protocol in the "Guidelines for Data Breach Handling" will, insofar as applicable, apply to the handling of such reported cases.

13.3 Investigation of the cases referred to above will be done in an impartial and efficient manner, and a report will be submitted to the Compliance Committee for consideration.

14. Communications and Enquiries

14.1 Any question by employees regarding:

14.1.1 this Policy should be addressed to the DPO;

14.1.2 the PMP program control measures for customer personal data and employee personal data should be addressed to the Customer Personal Data Protection Officer and Employee Personal Data Protection Officer respectively; and

14.1.3 the BU's policy or practice on personal data protection should be addressed to the BU Head or the BU Personal Data Coordinator.

14.2 External complaints or enquiries regarding personal data privacy matters should be handled in accordance with the "Guidelines for Personal Data Privacy Complaints and Enquiries Handling" issued by the DPO.

- E N D -