Power Assets Holdings Ltd.
電能實業有限公司

Personal Data Privacy Policy

October 2020

Table of Contents

1. Introduction

1.1 Power Assets Holdings Limited and its subsidiaries (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 (Chapter 486 of Laws of Hong Kong) 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 The Group may also be subject to privacy laws applicable in other jurisdictions (together with the Ordinance, the "**Privacy Laws**") where its operating companies are established such as the European Union countries, Mainland China, Australia, New Zealand and Canada etc. In particular, when the Group processes personal data received from its operating companies that are based in countries such as the European Union countries, it may be subject to the European Union General Data Protection Regulation. In all cases, the Group needs to ensure compliance with these Privacy Laws and any relevant guidelines published by the relevant authorities for compliance with Privacy Laws, as applicable to the personal data processes the Group may undertake from time to time.

1.3 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 should also observe any additional personal data policies, rules, regulations, requirements and guidelines to which they may be subject from time to time. It also applies to all employees of The Hongkong Electric Company, Limited, a wholly-owned subsidiary of HK Electric Investments Limited, to the extent that they are providing support services to the Group.

1.4 It is a joint effort by all to ensure that the relevant Privacy Laws 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, shareholders, visitors, job applicants, employees, other stakeholders and persons involved in our businesses. Violation of the Privacy Laws may result in civil or criminal sanctions, as well as serious harm to the Group's reputation.

1.5 Non-compliance of 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 functional unit 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 should 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
(DPP 4 – 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
(DPP 6 – 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.

10.2 Each functional unit of the Group (e.g. Power Assets Investments Limited, Associated Technical Services Limited, legal, company secretarial, financial, accounting, treasury, internal audit, human resources, public affairs, corporate development, information technology and administrative services etc.) should maintain a register of data processors and/or third party service providers having access to the personal data under the functional unit's control and custody, and identify the 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 Heads of the functional units are responsible for assessing whether any of its business activities constitutes a direct marketing activity.

11.4 Each functional unit 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. Processing of Personal Data received from Relevant Operating Companies

Insofar as the Group's processing of personal data received from its overseas operating companies, the Group should follow the "Guidelines for Compliance with Privacy Laws (relating to processing of personal data received from Relevant Operating Companies)" and any other guidelines issued pursuant to paragraph 13.3.

13. Personal Data Protection Officer

13.1 The Group Legal Counsel and Company Secretary is the Personal Data Protection Officer (the "**DPO**"), responsible for facilitating the Group's compliance of applicable Privacy Laws.

13.2 The DPO is responsible for:

13.2.1 the monitoring of the Group's compliance of the Ordinance and other applicable Privacy Laws;

13.2.2 the development and implementation of the programme controls and their ongoing assessment and revision;

13.2.3 the development on an oversight and review plan on a periodic basis that sets out how the effectiveness of the Group's programme controls will be monitored and assessed;

13.2.4 the recommendations to revisions to this Policy;

13.2.5 assisting in the investigations, where appropriate, on violation or suspected violation of this Policy or Privacy Laws; and

13.2.6 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.

13.3 For the purpose of discharging his/her responsibilities referred to above, the DPO may issue and/or update guidelines (including with limitation, updating the "Guidelines for Compliance with Privacy Laws (relating to processing of personal data received from Relevant Operating Companies") from time to time as he/she deems necessary.

13.4 The DPO is responsible for reporting the compliance status to the Governance and Compliance Committee of the Group.

14. Heads of Functional Units and FU Personal Data Coordinator

Heads of Functional Units

14.1 Heads of functional units have the primary responsibility to ensure their functional units' compliance with the Ordinance, other applicable Privacy Laws and this Policy, identify the inventory of personal data collected by their functional units, 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 other applicable Privacy Laws and give effect to this Policy.

14.2 When devising personal data protection measures, heads of functional units 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 functional units' policies and practice.

FU Personal Data Coordinator

14.3 Each functional unit should appoint a coordinator (the "**FU Personal Data Coordinator**") to liaise and communicate, as the functional unit's representative, with the DPO regarding the status of compliance of the Ordinance and applicable Privacy Laws and this Policy, and to support the heads of functional units in the discharge of their responsibilities. A head of functional unit can act as the FU Personal Data Coordinator, if considered to be appropriate.

14.4 The FU Personal Data Coordinators' roles include:

14.4.1 conducting periodic review and updates of the personal data inventory of their respective functional units;

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

14.4.3 arranging training on personal data protection for his/her functional unit to ensure compliance of the Ordinance and other applicable Privacy Laws and, where appropriate, seek assistance from the DPO to arrange training on specific topics.

15. Breach Handling and Reporting

15.1 Employees should be alert and vigilant with respect to any violation or suspected violation of personal data protection. Any breach or suspected breach of personal data protection or this Policy should be immediately reported to any of the head of the functional units, the DPO or the head of the functional unit in charge of internal audit. It can also be reported to the Group's whistleblower hotline.

15.2 The head of the relevant functional unit will investigate the report of breach or suspected breach and, to the extent appropriate, will be assisted by the DPO and/or the functional unit in charge of internal audit. Investigation will be done in an impartial and efficient manner, and a report will be submitted to the Chief Executive Officer and all members of the Governance and Compliance Committee for consideration of the follow up actions. Nevertheless, for any breach or suspected breach reported to the Group's whistleblower hotline, it will be handled in accordance with the relevant whistleblower investigation protocol.

15.3 All functional units have the responsibility to keep a register recording both breach and suspected breach of personal data protection, and the DPO will maintain a register of all reported breach and suspected breach.

16. Communications, Enquiries and Complaints

16.1 Any question regarding this Policy should be addressed to the DPO.

16.2 Any question on the functional unit's policy or practice on personal data protection should be addressed to the heads of functional units or the FU Personal Data Coordinators.

16.3 For general external enquiries or complaints regarding personal data privacy matters, the functional unit receiving such enquiries or complaints should forthwith notify the DPO and be responsible for their handling and response, taking into consideration any advice or guidance from the DPO.

- E N D -