AP&R PDPA Policy

Overview of the PDPA

The PDPA governs the collection, use and disclosure of individuals' personal data by organizations in a manner that recognizes both the right of individuals to protect their personal data and the need of organizations to collect, use and disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances. The PDPA contains two (2) main sets of provisions, covering data protection and the Do Not Call registry, which organizations are required to comply with.

The PDPA's data protection obligations are set out in Parts III to VI of the PDPA (the "Data Protection Provisions"). In brief, the Data Protection Provisions deal with the following matters:

a) Having reasonable purposes, notifying purposes and obtaining consent for the collection, use or disclosure of personal data;
b) Allowing individuals to access and correct their personal data;
c) Taking care of personal data (which relates to ensuring accuracy), protecting personal data (including protection in the case of international transfers) and not retaining personal data if no longer needed; and
d) Having policies and practices to comply with the PDPA.

There are 9 Personal Data Protection Obligations, and our Policy is developed based on these obligations.

Consent, Purpose Limitation and Notification Obligations

1. We collect personal data about our employees, such as:
   - Full name
   - NRIC or FIN number
   - Passport number
   - Photograph image
   - Mobile telephone number
   - Personal email address
   - Name and residential address
   - Name and residential telephone number

2. The purpose of collecting personal data is as below.
   - Employment application
   - For submissions to
     - IRAS (Inland Revenue Authority of Singapore)

- MOM (Ministry of Manpower) for Employment Pass Only
- Insurance Companies for the purpose of Group Employees Insurance Coverage
- CPF (Central Provident Fund Board)
- Banks

3. Consent is sought from employees during filling of application forms for new applicants and Consent Form for existing staffs.

4. Staff are also required to sign an undertaking in their handling of personal data in their course of work.

5. The use and disclosure of personal data is for administrative / statistical / risk management purposes.

Access & Correction Obligations

6. Procedure for staff to request for access to their personal data:
   - Request can be made via sending an email to Data Protection Officer ("DPO"); and
   - DPO can prepare document(s) in PDF format, encrypt with Password and return the email to sender.

7. Procedure for staff to request for changes in the personal data:
   - Request can be made via filling the "PERSONAL PARTICULARS UPDATE FORM", encrypt with Password and send to DPO via email for update; and
   - DPO can prepare document(s) in PDF format for the changed of personal data, encrypt with Password and return the email to sender for confirmation.

Accuracy Obligation

8. DPO will verify that the declaration clause to give accurate information in the application form is signed.

9. DPO will verify personal data given in accordance to the supporting documents, such as, IC for change of home address.

Protection Obligation

10. Personal data can only be accessed by DPO.

11. For soft copy of the personal data, they are stored with the DPO's notebook which is password protected.

12. Any sensitive document(s) will be encrypted with Password before sending out via email.

13. Notebook will be locked when staff is to walk away.

14. External parties will be escorted. And staff will be informed to keep personal data out of sight.

Retention Limitation Obligation

15. Our retention policy requires soft and hard copies of personal data to be disposed of by deletion and shredding respectively, after the retention period.

Transfer Limitation Obligation

16. We do not transfer personal data overseas.

Openness Obligation

17. Data protection polices will be briefed to all staff especially for DPO who handle personal data.

18. DPO's email is published in the AP&R's website for handling any queries relating to PDPA.

Data Intermediary

19. We do not process personal data on behalf of another organization, and as such AP&R is not a data intermediary.

DNC Registry

20. We do not perform tele marketing and therefore AP&R does not need to check with DNS registry.