港燈 HK Electric

135+ 推動永續未來 POWERING FOR SUSTAINABILITY

2 December 2025

Experience Sharing on Data Governance at HK Electric

LEUNG Wai-kin, General Manager (Customer Services), HK Electric

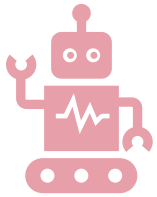
Strategies for Proactive & Effective Data Governance

Comprehensive Framework

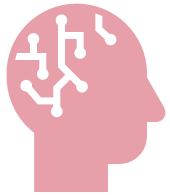
Clear Roles & Accountability

Preventive Controls

Continuous Monitoring



Automation & Innovation



Education & Culture

Strategies for Proactive & Effective Data Governance

Comprehensive Framework

- **Personal Data Privacy Policy** was first established in 2014, with the latest update released in 2020.
- A **Privacy Management Programme (PMP)** was introduced in 2020, providing comprehensive guidelines and documentation for assessment, data processor management, data breach handling and response, enquiry handling, and training.
- A **regularly updated Personal Data Inventory** is maintained for each business unit (BU) to manage the entire data lifecycle, from collection through to disposal.

Clear Roles & Accountability

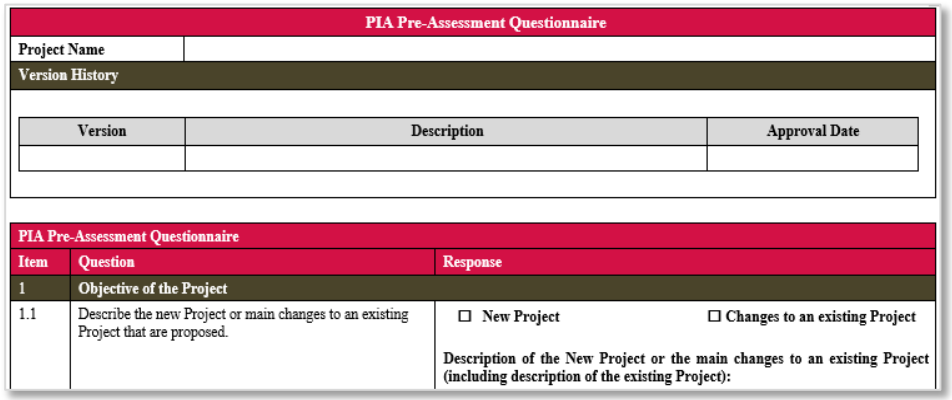
- Personal Data Protection Officer, Customer Personal Data Protection Officer, Employee Personal Data Protection Officer, BU Heads and BU Personal Data Coordinators worked together on privacy matters.
- Their roles and responsibilities are clearly documented.

Customer Services Division (Common Items) Last Revision: 31 Dec 2024					
Business Process	**Recruitment**	**Absence management (Sick Leave)**	**Absence management (Other Types of Leave e.g. Marriage Leave, Maternity**	**Absence management (Medical Consultation)**	**Commendation Form or Commendation Letter**
Type of Document	Electronic Record (emails/files on the following areas): - Shortlisted applicants - Interview schedule - Completed written test/ test result - Completed Interview Assessment Form Hardcopy: - Interview Assessment Form signed by interviewer - Completed written test scored by the interviewer	Hardcopy: For staff: Leave request/application form For workmen: 員工假期申請表 Sick leave certificate from staff & workmen	Hardcopy: For staff: Leave request/application form For workmen: 員工假期申請表 Leave certificate/supporting document from staff & workmen	Hardcopy: Clinic attendance certificate from staff & workmen	Hardcopy & Electronic Record Customers' commendation for our staff
Type of Personal Data	Applicant name, work experience, skills, education attainment, test result, comments by interviewer, salary information	Sick leave period, number of sick leave days, type of sickness	Type of leave, leave period, number of leave days and other personal data from the leave certificate/supporting document	Type of sickness	Name, address, telephone number, email address and signature of customer as well as name of the staff member
Data Subject	Job applicant	Employees	Employees	Employees	Customers
Data User	Hiring Division/Department and HR	Sick Leave Record of Staff - CS Division/ Department/ Section Heads - The Time & Leave Administrator (TLA) of CS Division (i.e. GMCS Secretary) - The Time & Leave Administrators (TLAs) at Department/Section level Sick Leave Record of Workmen - CS Division/ Department/ Section	Leave Record of Staff - CS Division/ Department/ Section Heads - The Time & Leave Administrator (TLA) of CS Division (i.e. GMCS Secretary) - The Time & Leave Administrators (TLAs) at Department/Section level Leave Record of Workmen - CS Division/ Department/ Section	Medical Consultation Record of Staff - CS Division/ Department/ Section Heads - The respective handlers of clinic attendance certificate Medical Consultation Record of Workmen - CS Division/ Department/ Section Heads	Authorized users in CS Division

Strategies for Proactive & Effective Data Governance

Preventive Controls

- **The Information Security Policy,** along with specific policies such as the Password Policy and Mobile Device Policy, sets out IT provisions and preventive controls to safeguard personal data privacy and maintain data confidentiality.
- **Privacy Impact Assessments** are conducted to evaluate privacy risks for new or enhanced processes that involve personal data.



PIA Pre-Assessment Questionnaire		
Project Name		
Version History		
Version	Description	Approval Date

PIA Pre-Assessment Questionnaire		
Item	Question	Response
1	Objective of the Project	
1.1	Describe the new Project or main changes to an existing Project that are proposed.	☐ New Project ☐ Changes to an existing Project Description of the New Project or the main changes to an existing Project (including description of the existing Project):

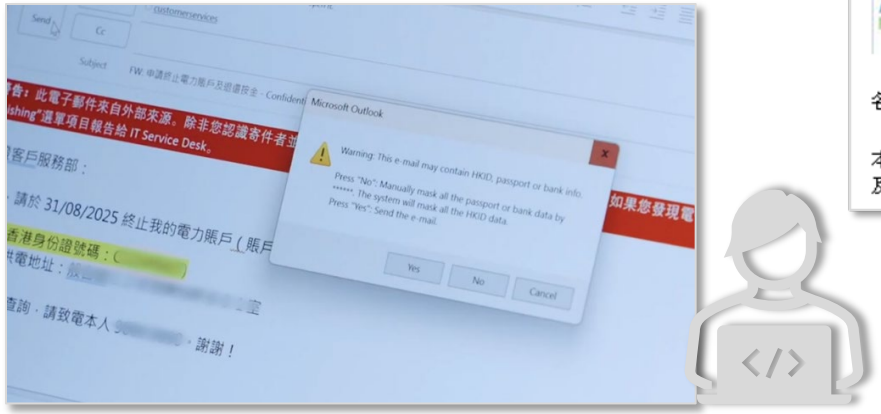
Continuous Monitoring

- **Data Loss Prevention System**: Protects against intentional and unintentional disclosure of personal data via the Internet, email, portal storage devices, and file transfers.
- **Security Incident Monitoring**: Centralises log collection and analyses patterns to detect anomalies and potential breaches.
- **Vulnerability Scanning & Penetration Testing**: Regularly identifies and remediates weaknesses proactively.
- **Audit & Compliance Reviews**: Conducts periodic internal audits and external ISO audits to validate the effectiveness of risk management.

Strategies for Proactive & Effective Data Governance

Automation & Innovation

- Adopt a single-copy paperless approach to confine the risk of personal data privacy.
- Automatic deletion of time-expired records containing personal data, with alerts and logging.
- Automatic masking of HKID numbers in outgoing emails using end-user computing tools.



Education & Culture

- Privacy Awareness Week.
- Regular cybersecurity and information security awareness training and quizzes.
- Training for new joiners and regular phishing drills.

Privacy by Design

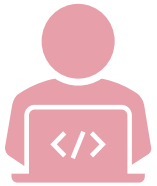
Privacy embedded in the smart metering system from the outset.

Smart meters collect electricity consumption data for every thirty minutes enabling customers to manage their energy usage via Account-On-Line portal.

A comprehensive **Privacy Impact Assessment (PIA)** was carried out by a reputable independent assessor before the start of the project.

End-to-end encryption is used to secure data transmission from smart meters to HK Electric's meter data hubs.

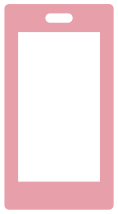
Data minimisation is applied across various meter data hubs to ensure that no customer personal data is stored.



Stringent access controls are applied to these data hubs, following the need-to-know principle.

Privacy by Default

Privacy-friendly settings are enabled automatically.

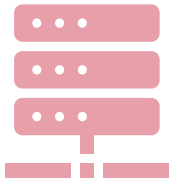


Notification Settings on HK Electric App

Notifications are disabled by default, and customers can enable push notifications for news updates and promotional offers at their discretion.

E-Form Confirmation Emails

HKID card information is automatically masked in confirmation emails sent to customers.



Single Repository

All incoming emails, e-forms, and faxes will be stored in a single repository and automatically tagged with labels to indicate the presence of personal data, where appropriate.

Enquiry, Fax and Postal Records on SharePoint

The SharePoint sites used to maintain enquiry logs, incoming faxes, and postal correspondence are configured to automatically delete records from the portal after the defined retention period.

Privacy Controls & Measures to Enhance Data Security

Access Control

Role-based access control, adherence to the least privilege principle, and implementation of multi-factor authentication (MFA).

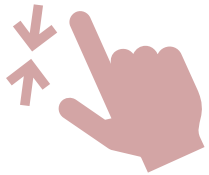
Data Masking

Customer information is masked after a defined period following account closure.

Data Lifecycle Management

Define retention periods and automate secure deletion of outdated data.

Underlying Philosophies



Minimalism

Collect and retain only the minimum personal data necessary.

Single Copy

Keep a single copy of documents or correspondence containing personal data in one repository, with appropriate access controls and a defined retention policy.

Preparation for Future Privacy Challenges

- **Operations in Clouds**
  - Select secure cloud platforms with built-in retention policies and robust authorisation settings to ensure compliance and controlled access.
  - Establish clear demarcation of responsibilities and controllable areas between all parties.
- **Regular Security Reviews & Audits**
  - Conduct regular reviews of the latest available technologies to be deployed within the company for operations or for safeguarding personal data privacy.
  - Perform regular audits to ensure compliance with defined policies and guidelines.
- **Potentials and Risks with Artificial Intelligence (AI)**
  - Assess the feasibility of deploying AI in areas such as data discovery and classification, anomaly detection, automated compliance monitoring, data minimisation and masking, intelligent access control, secure data sharing and incident response automation.
  - Consider risks associated with AI, such as inadvertent sharing of personal data through underlying learning models.

Thank you