PRUDENTIAL
保 誠 保 險

Effective Data Governance in Action

Experience Sharing Session by Privacy-Friendly Awardees 2025

Speaker: Pele Cheung
Director, Business Information Security Office

Practical strategies for implementing proactive and effective data governance to manage and safeguard sensitive customers' personal data at scale
推行積極高效的數據管治的實務策略，以妥善處理及保障大量敏感的客戶個人資料

Privacy controls/measures taken to enhance data security in response to emerging privacy challenges
為提升數據安全及應對未來私隱挑戰所採取的私隱保障措施

How to leverage technology for privacy protection
如何借助科技提升私隱保障

Data Governance Framework

Data Governance Framework

Policy	**Rules for managing data**
People	**Clear ownership with defined roles**
Process	**Standardised data lifecycle workflows**
Technology	**Automated discovery and monitoring**

Policy

- Identify applicable regulatory and legal requirements
- Define lawful purposes and retention periods for data
- Ensure data usage aligns with stated policies and notices
- Conduct regular compliance reviews and audits
- Maintain documentation and evidence for regulatory accountability

People

- Data Owner – Accountable for data and risk
- Data Steward – Manages and governs data quality and usage
- Data Custodian – Protects and operates data technically
- Data User – Uses data responsibly for approved purposes

Process

- Define and standardise data lifecycle management (collect, use, store, delete)
- Establish data classification and handling rules based on risk
- Ensure data quality controls and issue remediation
- Govern data access, usage, and sharing, including third parties
- Embed privacy, security, incident handling, and continuous review into operations

Technology

- Enable data discovery, inventory, and classification across systems
- Enforce access control and identity management using least-privilege principles
- Implement data protection controls (encryption, masking, backup, recovery)
- Provide monitoring, logging, and Data Leakage Prevention to detect and prevent data misuse
- Automate data lifecycle management, including retention, archiving, and deletion

Policy

- Identify applicable regulatory and legal requirements
- Define lawful purposes and retention periods for data
- Ensure data usage aligns with stated policies and notices
- Conduct regular compliance reviews and audits
- Maintain documentation and evidence for regulatory accountability

People

- Data Owner – Accountable for data and risk
- Data Steward – Manages and governs data quality and usage
- Data Custodian – Protects and operates data technically
- Data User – Uses data responsibly for approved purposes

Process

- Define and standardise data lifecycle management (collect, use, store, delete)
- Establish data classification and handling rules based on risk
- Ensure data quality controls and issue remediation
- Govern data access, usage, and sharing, including third parties
- Embed privacy, security, incident handling, and continuous review into operations

Technology

- Enable data discovery, inventory, and classification across systems
- Enforce access control and identity management using least-privilege principles
- Implement data protection controls (encryption, masking, backup, recovery)
- Provide monitoring, logging, and Data Leakage Prevention to detect and prevent data misuse
- Automate data lifecycle management, including retention, archiving, and deletion

Policy

- Identify applicable regulatory and legal requirements
- Define lawful purposes and retention periods for data
- Ensure data usage aligns with stated policies and notices
- Conduct regular compliance reviews and audits
- Maintain documentation and evidence for regulatory accountability

People

- Data Owner – Accountable for data and risk
- Data Steward – Manages and governs data quality and usage
- Data Custodian – Protects and operates data technically
- Data User – Uses data responsibly for approved purposes

Process

- Define and standardise data lifecycle management (collect, use, store, delete)
- Establish data classification and handling rules based on risk
- Ensure data quality controls and issue remediation
- Govern data access, usage, and sharing, including third parties
- Embed privacy, security, incident handling, and continuous review into operations

Technology

- Enable data discovery, inventory, and classification across systems
- Enforce access control and identity management using least-privilege principles
- Implement data protection controls (encryption, masking, backup, recovery)
- Provide monitoring, logging, and Data Leakage Prevention to detect and prevent data misuse
- Automate data lifecycle management, including retention, archiving, and deletion

Policy

- Identify applicable regulatory and legal requirements
- Define lawful purposes and retention periods for data
- Ensure data usage aligns with stated policies and notices
- Conduct regular compliance reviews and audits
- Maintain documentation and evidence for regulatory accountability

People

- Data Owner – Accountable for data and risk
- Data Steward – Manages and governs data quality and usage
- Data Custodian – Protects and operates data technically
- Data User – Uses data responsibly for approved purposes

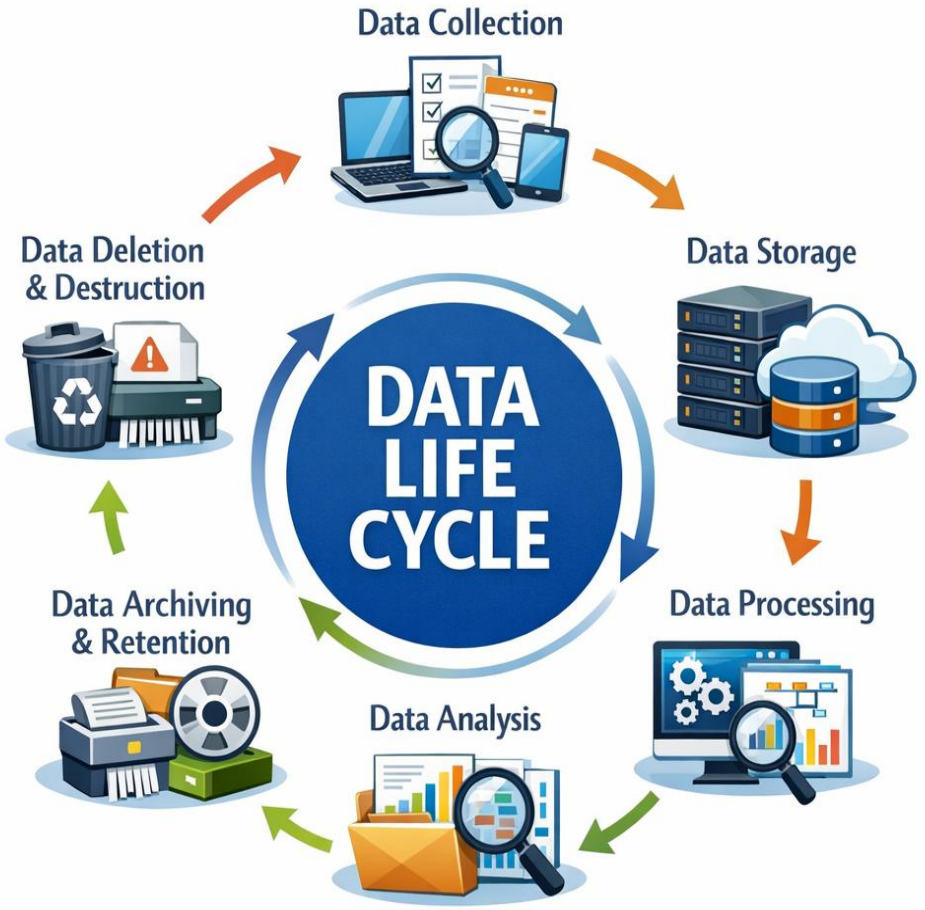
Process

- Define and standardise data lifecycle management (collect, use, store, delete)
- Establish data classification and handling rules based on risk
- Ensure data quality controls and issue remediation
- Govern data access, usage, and sharing, including third parties
- Embed privacy, security, incident handling, and continuous review into operations

Technology

- Enable data discovery, inventory, and classification across systems
- Enforce access control and identity management using least-privilege principles
- Implement data protection controls (encryption, masking, backup, recovery)
- Provide monitoring, logging, and Data Leakage Prevention to detect and prevent data misuse
- Automate data lifecycle management, including retention, archiving, and deletion

Data Life Cycle



Key focus

- Legitimacy & Purpose – Data is collected for clear, lawful, and defined business purposes
- Data Minimisation – Only necessary and relevant data is collected
- Accuracy & Quality – Data is correct, complete, and fit for use
- Transparency & Consent – Individuals are informed and consent is obtained where required
- Security at Entry Point – Data is protected at the point of capture
- Regulatory Compliance – Collection complies with applicable laws, regulations, and policies

Key focus

- Confidentiality & Security – Data is protected against unauthorised access and breaches
- Integrity – Data remains accurate, complete, and unaltered during storage
- Availability & Resilience – Data is accessible when needed and protected against loss
- Compliance – Storage meets legal, regulatory, and policy requirements
- Location & Residency – Data is stored in approved locations (on-perm / cloud / region)
- Lifecycle Alignment – Storage supports retention, archiving, and deletion requirements

Key focus

- Purpose Limitation – Data is processed strictly for approved and defined purposes
- Accuracy & Data Quality – Processed data remains correct, consistent, and reliable
- Privacy & Confidentiality – Personal and sensitive data is protected during processing
- Security Controls – Processing activities are safeguarded against unauthorised access or misuse
- Compliance – Processing complies with applicable laws, regulations, and internal policies
- Traceability & Accountability – Processing activities are documented and auditable

Key focus

- Purpose Alignment – Analysis is conducted for approved, legitimate business objectives
- Data Quality & Reliability – Analysis is based on accurate, complete, and trusted data
- Privacy & Confidentiality – Personal and sensitive data is protected during analysis
- Security of Analytical Environment – Analytical tools and platforms are securely controlled
- Fairness & Ethics – Analysis avoids bias, misuse, or unethical customers (especially for AI/advanced analytics)
- Accountability & Transparency – Analytical assumptions, logic, and outputs are explainable and auditable

Key focus

- Regulatory & Policy Compliance – Data is retained in accordance with legal, regulatory, and policy requirements
- Data Minimisation – Data is retained only for as necessary
- Security of Archived Data – Archived data remains protected from unauthorised access or loss
- Integrity & Authenticity – Archived data remains accurate, complete, and tamper-proof
- Accessibility & Recoverability – Archived data can be retrieved when required
- Clear Accountability – Ownership and responsibility for retained data are clearly defined

Key focus

- Regulatory & Policy Compliance – Data is deleted in accordance with retention schedules and legal requirements
- Data Minimisation – Data is permanently removed once it is no longer required
- Irreversibility – Deleted data cannot be recovered or reconstructed
- Security Assurance - Deletion methods prevent unauthorised recovery or data leakage
- Consistency Across Media – Data is securely removed from all systems, backups, and physical media
- Accountability & Auditability – Deletion activities are authorised, documented, and verifiable

Technology for Privacy Protection

Data Leakage Prevention (DLP)

Identity Access Management (IAM)

Endpoint Detection and Response (EDR)

Data Leakage Prevention

Data Identification & Classification
- Identify sensitive data
- Apply consistent data classification and labelling standards

Policy Definition & Governance
- Define DLP policies aligned with regulatory and business requirements
- Set clear rules for data handling, sharing and transfer

Monitoring & Detection
- Monitor data in use, in motion, and at rest across endpoints, email, cloud and network
- Detect unauthorised access or sharing

Preventive Controls
- Enforce controls such as blocking, quarantining, encryption
- Apply least-privilege access and conditional controls based on risk

Identity Access Management

Strong Authentication (Multi-factor authentication)

- Enforce MFA for privileged, remote and sensitive system access
- Apply risk based or adaptive authentication
- Disable legacy or weak authentication protocols
- Regularly review MFA coverage and exceptions

User Access Provisioning & De-Provisioning

- Integrate IAM with HR systems where possible
- Immediately revoke access upon termination or role change
- Validate access request against approved roles and data classifications
- Define and maintain business-aligned roles and role matrices (Role Based Access Control)
- Prevent ad-hoc or direct user-level entitlements

Privileged Access Management (PAM)

- Vault and rotate privileged credentials
- Enforce session monitoring and logging
- Restrict direct admin access to production systems
- Review privileged account usage regularly

Endpoint Detection & Response

Threat Detection & Behavioural Monitoring
- Detect malware, ransomware attack
- Identify suspicious data access or mass file operations
- User behaviour based detection beyond signature matching

Data Exfiltration & Leakage Detection
- Monitor unusual outbound network connections
- Detect abnormal use of removable media
- Flag unauthorised data compression, encryption or bulk transfer
- Correlate endpoint activity with DLP and network controls

Ransomware & Data Destruction Protection
- Detect early indicators of ransomware behaviour
- Automatically stop file-encryption processes
- Trigger immediate containment on ransomware detection