Experience Sharing on Data Governance

Dickson Lau
Data Protection Officer

Agenda

1

Practical experience in setting up a Personal Data Privacy Management Programme

Why Is a Privacy Governance Model Important?

Drivers

1. **Need For A Unified Privacy Governance & Compliance Model for Businesses In The Global Market**

2. **More Stringent Laws, Higher Penalties & Damages**

3. **The Industry Is Facing Challenges In Data Protection & Privacy Compliance**

With the increasing commercial value of personal information, security crises also follow suit. We are facing privacy compliance risks at various stages of the data lifecycle.

Data security of confidential data and cross-border compliance

Having the potential to collect and generate data that may fall into categories identified as important or sensitive. Examples included but not limited to:

1. Important Data
   - Sales and distribution data (I.e. Sales figure, distribution routes and retail outlet information)
   - Production and inventory information (i.e. batch no, manufacturing process data and supply chain data)
2. Sensitive Data
   - Consumer data and preference
   - B2B Customer Data
   - Employee personal data
   - Payment and financial data

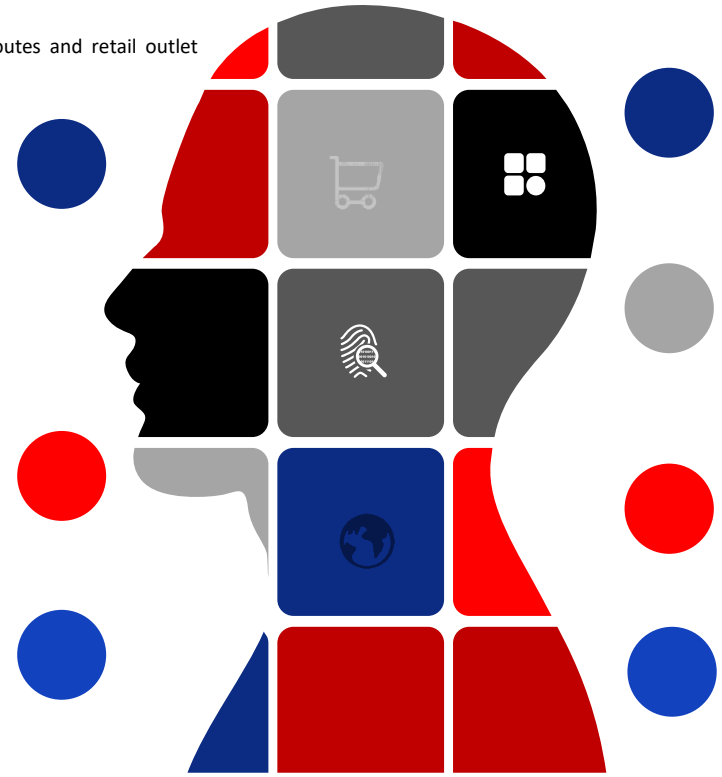
The handling of confidential data in industry might subject to tighter control in cross-border scenarios.

Third Party Data Risk

When engaging with third parties for activities such as collecting personal information, outsourcing data processing, utilizing products or services from third-party providers, or transmitting personal information to external entities, it is crucial to address data compliance and security risks associated with these third-party interactions.

Excessive Personal Data Collection

The processing of personal data should be appropriate, relevant, and necessary to fulfill the purpose, however, it could still potentially result in an excessive amount of data, which does not align with the principle of data minimization and poses compliance risks.



Privacy Compliance Risk (Data Collection)

Due to more stringent requirements upon collection of sensitive information, the industry will face significant attention regarding obtaining data subject's authorization and explicit consent for collecting information.

Privacy Compliance Risk (Data Storage & Retention)

If database lacks strong encryption measures, technical safeguards and data retention schedule, along with strict restrictions on access permissions, it becomes susceptible to exploitation by hackers

Privacy Compliance Risk (Data Transmission)

The transmission of personal sensitive information without encryption has significant impact on security of sensitive information.

Privacy Compliance Risk (Data Usage)

Sensitive information scattered across different systems within the enterprise might lack proper access control measures. Data subject might not be granted rights to inquire, correct or delete their personal information.

Why Is a Privacy Governance Model Important?

1 Miss Out Business Opportunities

- Absence of privacy guidelines and SOP face challenges to support new business initiatives
- E.g. Use of AI and ChatGPT technologies

2 Pose Potential Loss

- Lack of compliance with the local regulations may result in:
  - Law violation
  - Cost Incurrence
  - Brand and Reputation Damage

3 Impact Existing Running Project or Systems

- Significant gap might affect functionality and efficiency of existing system
- Overlook potential privacy risk leading to infringe on privacy laws
- Lead to unregulated handling of data, potentially resulting in data misuse.

4 Create Gaps with Business Strategy

- Absence of a standardized privacy SOP for governing and monitoring business processes can lead to suspension of certain activities

SCC Personal Data Privacy Management Programme (PDPMP) Journey

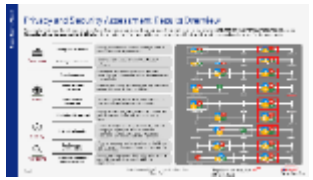
SCC Privacy Programme Maturity Journey

Assess Current Capabilities | **Design Future State** | **Operate and Sustain**

2020 | **2021 – 2022** | **2023 and Beyond**

Current state analysis and data discovery

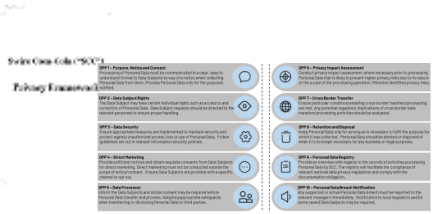
- As-is business practices and operations understanding
- Data flow and inventory discovery



Privacy maturity assessment

Gap assessment and remediation roadmap

- Identify and prioritize gaps between as-is and to-be state
- Propose remediations and deliverables



Privacy Framework

Build foundation and programme planning

- Policy framework development
- Setup the foundation for privacy protection implementation

Privacy Notice Template and User Guide
Employee Code of Conduct, etc

Implementation and programme maturing

- Privacy protection policy and programme implementation
- ISO certifications for Chinese Mainland

Privacy Impact Assessment Questionnaire

Ongoing programme operation and monitoring

- Sustainable privacy practices
- Ongoing monitoring of privacy regulations development
- Privacy assessment automation
- ISO certifications for other regions

ISO 27701
ivacy Information Management

Top-down Approach to Set the Anchor

Management and Privacy Champions

Endorsement

InfoSec and Privacy Governance Committee

Train the Trainer

Privacy Champions

Training

Circulation

Workshops

Data Privacy Intranet Portal

Centralization

Privacy Management Platform

Continuous Communication

General Users

Training

Role-based Training

For specific user groups who handles large amount of Personal Data, or will be involved in the Privacy by Design process
i.e. HR Departments

Ease-of-Use

Ready-to-Use Templates

Customized templates such as Privacy Notice / PICS are designed to have minimal user interactions and readily accessible information for references

Practicality

Guidance and Handling Procedures

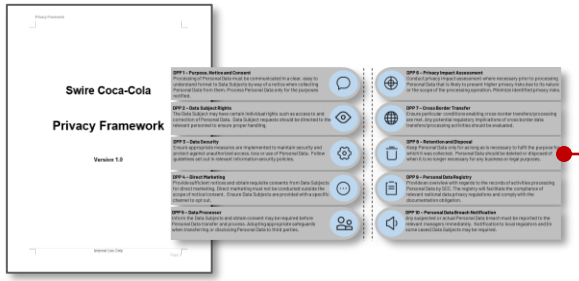
Practical guidelines and step-by-step handling procedures, with real-life case studies

Awareness

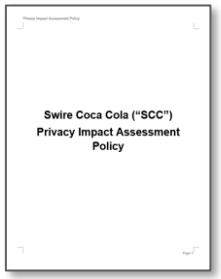
Multi-Media

Usage of posters, video, applications to increase awareness and understanding

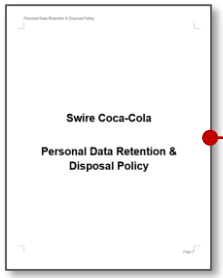
SCC Privacy Framework



Privacy Framework



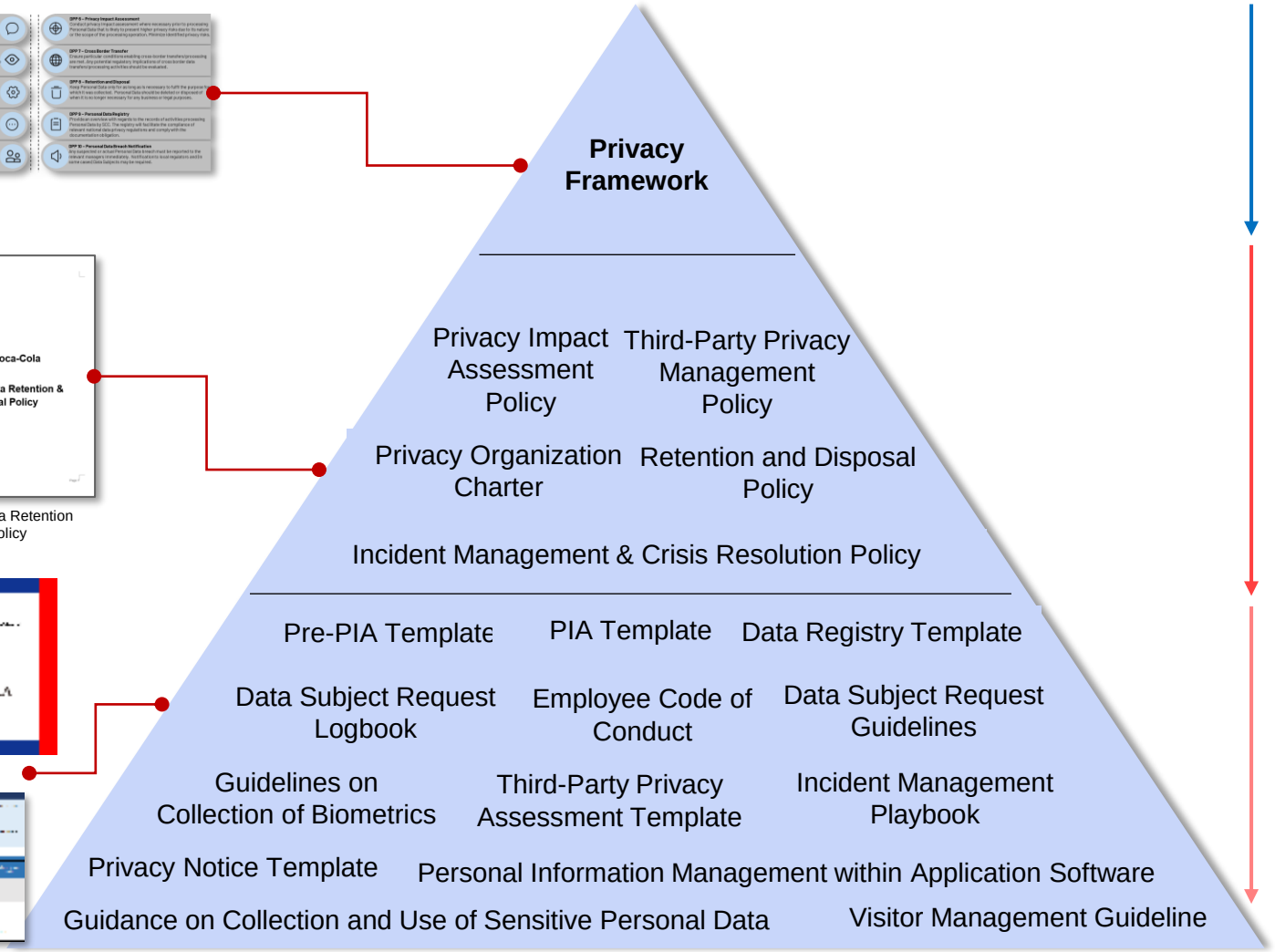
Privacy Impact Assessment Policy



Personal Data Retention & Disposal Policy

Privacy Impact Assessment Template

Data Registry Template



Part 1

Framework

Sets out the principles and requirements when collecting, processing or managing Personal Data

Part 2

Policies

Details the specific privacy requirements with respects to the Framework, pertaining to the specific area

Part 3

Guidelines, Templates and Procedural Documentation

Provides hands-on, practical guidelines and requirements, as well as ready-to-use templates for easy user adoption.

Adopting SCC Privacy Framework and Privacy Principles

SCC Privacy Framework
Overcharging anchor to set the baseline on SCC privacy expectation and strengthen users' knowledge and compliance obligations on data privacy.

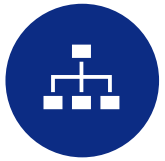
Country-specific definitions
Covers regulations and requirements from different regions

Privacy Principles
Contains 10 Key Data Privacy Principles ("DPPs") that must be followed

1. **Purpose, Notice and Consent**
   What should be communicated to the Data Subject before collecting his/her Personal Data
2. **Data Subject Rights**
   What are the individual rights of Data Subjects?
3. **Data Security**
   What security measures should be implemented? Are logical access controls sufficient?
4. **Direct Marketing**
   What are the considerations if Direct Marketing are involved?
5. **Data Processor Assessment and Data Processing Agreement (DPA)**
   Roles and Responsibilities of SCC if personal data would be shared or outsourced
6. **Privacy Impact Assessment**
   To systematically identify the risks and potential effects of collecting, maintaining, and disseminating PII and to examine and evaluate alternative processes for handling information to mitigate potential privacy risks.
7. **Cross Border Transfer**
   Considerations if such personal data were to be transferred outside of its country of origin
8. **Retention and Disposal**
   Considerations when retaining, or disposing personal data
9. **Personal Data Registry and Data Flow**
   An inventory and data flow of the data processing for having an overview of what we are doing with the concerned personal data
10. **Consent and Opt-out Management**
    What constitute as a consent, scenarios where explicit consent is required, Considerations when opt-out request is received

Key Policies and Guidelines

Privacy Framework
Overcharging anchor to set the baseline on SCC privacy expectation and strengthen users' knowledge and compliance obligations on data privacy.



Privacy Organizational Charter
Defines organization roles and responsibilities in privacy management.

Data Retention and Disposal Policy
Outlines key principles which govern the retention and disposal of Personal Data in SCC.

Privacy Incidents Management and Crisis Resolution
(with Incident Management Playbook)
An introduction of privacy incidents and changes to the existing incident management.

Data Subject Request Guidelines and Logbook
Provide guidance on how to handle data subject request and logbook template to record the data subject request.

Guidelines on Collection of Biometrics
Provide guidance on the collection and handling of sensitive biometrics data.

Privacy Impact Assessment Policy
(with Pre-PIA template, PIA template)
Policy and template to facilitate the identification of privacy risk in new or enhanced initiatives.

Third-Party Privacy Management Policy
(with Third-party privacy assessment template)
A comprehensive assessment to evaluate and monitor privacy risk of third party vendors processing personal data on behalf of SCC.

Data Registry and Data Flow Diagram Template
Record all of the personal data handled and act as a personal data inventory.

Data Classification Guideline
Classifying data based on its sensitivity, value and criticality to the company, so sensitive personal data can be secured appropriately.

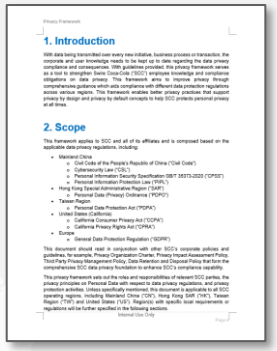
Employee Code of Conduct
To set out the expectation on data protection of each employee.

Privacy Notice Policy and Template
Easy-to-adopt template to be embedded in the personal data collection process.

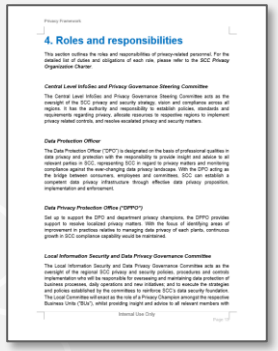
Tools for Privacy Governance

Privacy Framework

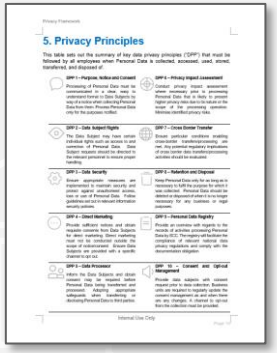
The Privacy Framework aims to improve privacy through comprehensive guidance which aids compliance with different data protection regulations across various regions and serves as a bare minimum requirement for employees to follow when collecting and handling personal data.



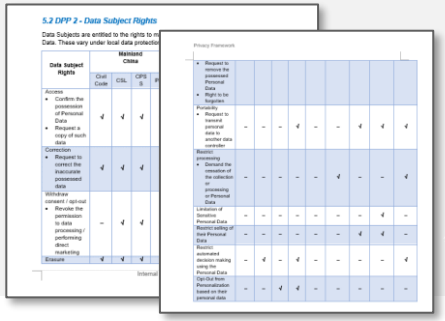
Scope has been defined within the framework, covering applicable laws and regulations such as CCPA, CPRA within US and PIPL within China.



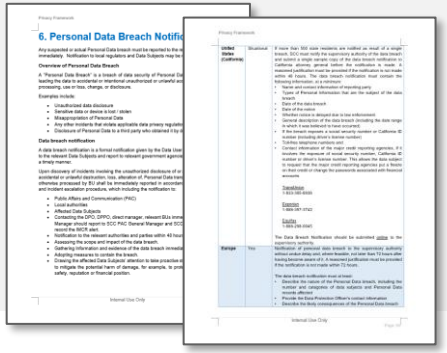
It defines roles and responsibilities for different stakeholders within SCC.



The Framework set out 10 data privacy principles (“DPP”) that must be followed by all employees when processing personal data.

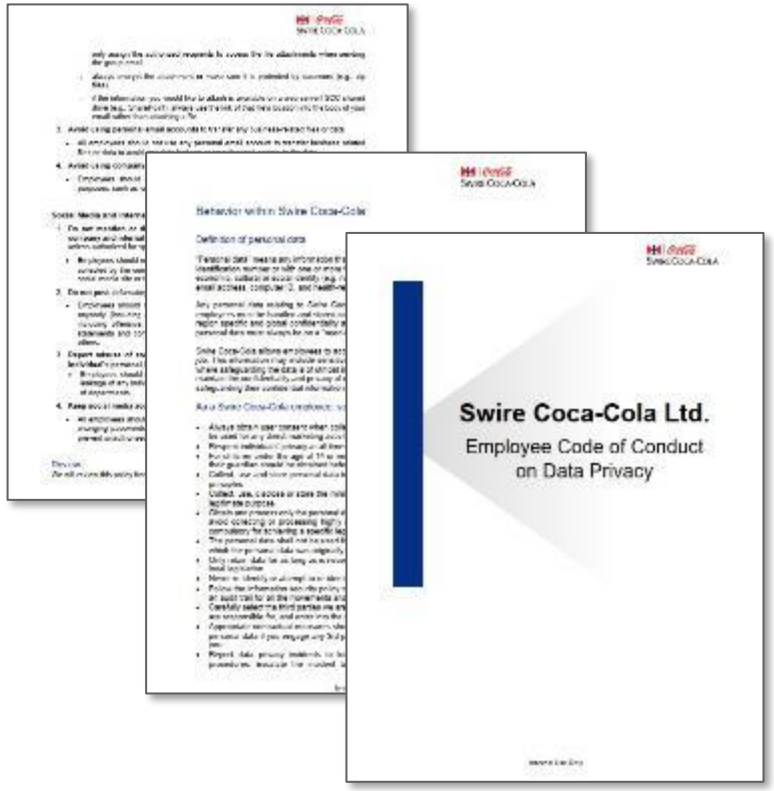


The Framework provides region specific requirements on areas such as Data Subject Rights and Content of Privacy Notice to accommodate the local business operations.



The section of Personal Data Breach Notification has been included which provides guidance to users in notifying local regulators as well as their data subjects, including the content and timeframe of such notification.

Employee Code of Conduct



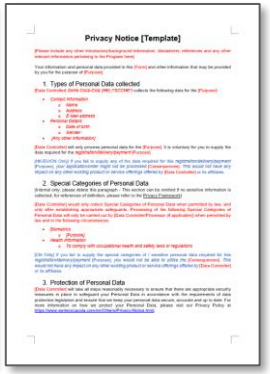
The Employee Code of Conduct explicitly sets out Dos and Don’ts that employees should adhere to from the perspective of data privacy.

Tools for Consent Management and DSAR

In order to manage consent from data subject access rights in an appropriate and effective manner, tools including Privacy Notice Template, Data Registry Template, as well as Tools for handling Data Subject Access Rights (DSAR) request including Handling Guideline and Request Form and Logbook have been established and rolled out to users.

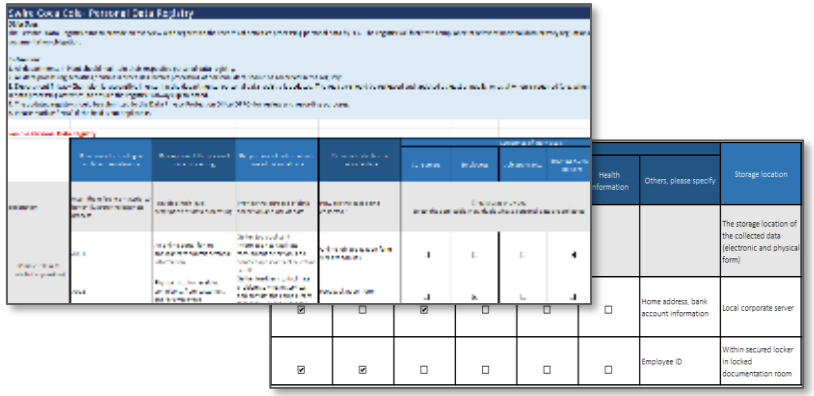
Privacy Notice Template

The Template allow users to customize their Privacy Notice according to the business needs to ensure consent would be obtained in an appropriate format and manner.



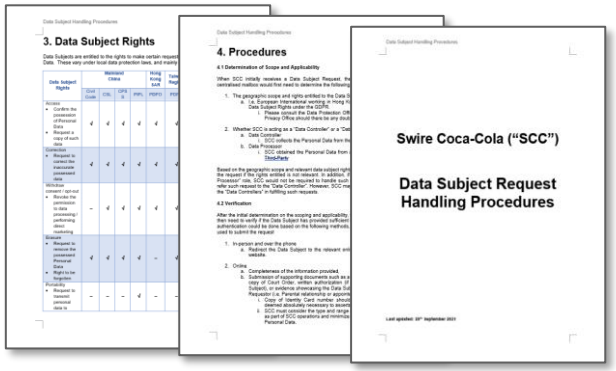
Data Registry Template

A database to record relevant details of the process that involves the collection, processing or retention of personal data

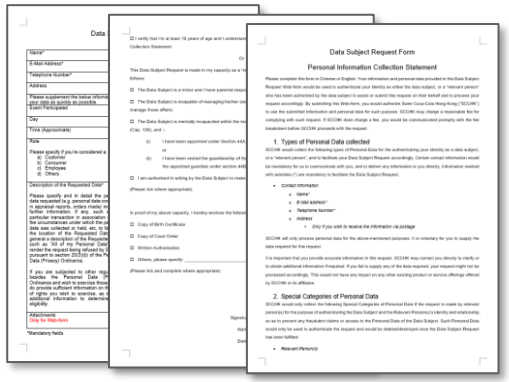


Tools for handling Data Subject Access Rights Request Guideline

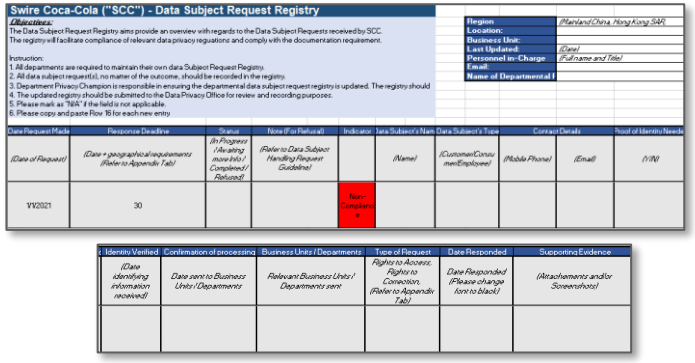
Tools for handling Data Subject Request including Handling Guideline and Request Form and Logbook have been established.



The **Data Subject Request Guideline** specify the rights data subjects are entitled to under different jurisdictions and stipulates the procedure of handling such request within certain timeframe.



The **Data Subject Request Form** provides a standardized channel for data subjects to exercise their rights.



The **Data Subject Logbook** is a database to record the received requests.

2

Privacy safeguards taken to protect personal data and ensure data security

Data Privacy Compliance  Data Security Measures

Data Privacy Compliance	Data Security Measures
Compliance with personal data protection laws and regulations Focusing on the rights of individuals, the purpose of data collection and processing, how to collect, process, share, archive, and delete the data in accordance with the law. Most common concerns regarding data privacy • Data registry (RoPA) and data classification • Privacy Impact Assessment (PIA) • Consents and Data Subject Access Rights • Managing contracts and third-party • Data retention and disposal • Cross border data transfer • Applying governing regulation and law	Measures that are taking in order to prevent any third party from unauthorized access Focusing on protecting personal data from any unauthorized third-party access or malicious attacks and exploitation of data. It is set up to protect personal data using different methods and techniques to ensure data privacy. Most common Data Security measures and practices can include: • Activity monitoring • Network security • Access control • Breach response • Encryption • DLP

Adopting privacy by design

A Privacy Impact Assessment (PIA) is a systematic and compliance tool used to evaluate the privacy risks of any new/changes to business operations that process Personal Identifiable Information (PII or Personal Data), covering the data lifecycle from collection, use and sharing, storage, retention to disposal, and to identify the potential control measures in order to mitigate the associated privacy risks.

Pre-Assessment

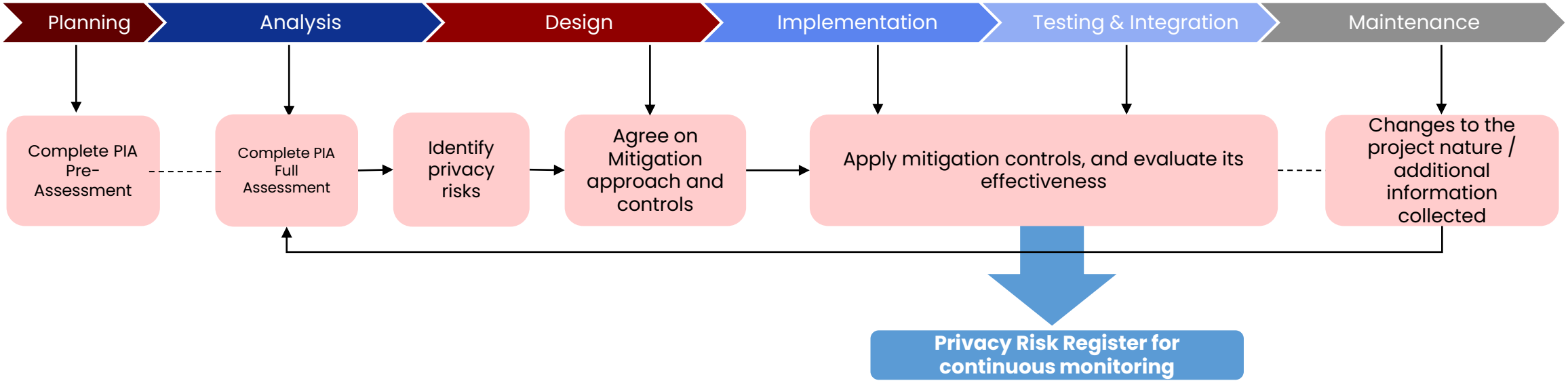
Screening mechanism to determine if additional PIA Full Assessment is necessary

PIA Full Assessment

Deep dive privacy assessment for all projects and initiatives involving processing of personal data to identify the privacy gaps and risks, determine appropriate mitigation action to minimize the privacy risk

How to perform a PIA?

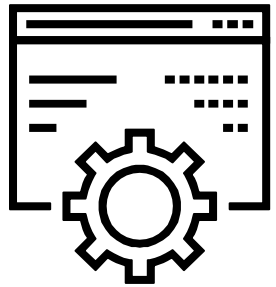
Product Development Life Cycle



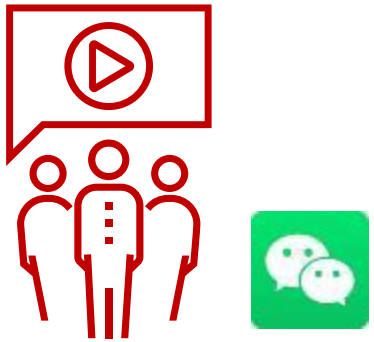
Conducting Data Privacy Training

It is essential to mature the concept of "privacy by design" among staff with top management support through various media, to emphasize how data privacy and protection can enhance business competitiveness while help strengthen the differentiating corporate branding. Below are some of the suggested activities:

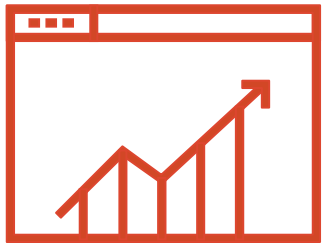
Staff onboarding awareness activities



Launch of Refreshed Privacy e-Learning and Newsletter



Company-wide privacy awareness communication and data breach incident response drill



Data Privacy Intranet Portal and e-Assessment Tool

Suggested privacy safeguards to protect personal data and ensure data security

- Data Encryption
- Access Control
- Secure Data Storage
- Regular Data Backups
- Employee Training and Awareness
- Data Minimization
- Privacy by Design
- Regular Security Audits and Assessments
- Third-Party Risk Management
- Compliance with Privacy Laws

Ongoing data privacy management operation model (Lifecycle)

Ongoing Data Privacy Management Operation Model

Process
- Standards & Guidelines
- Best Practices
- Internal Governance Structure

Technology

Personnel
- Experience
- Ability

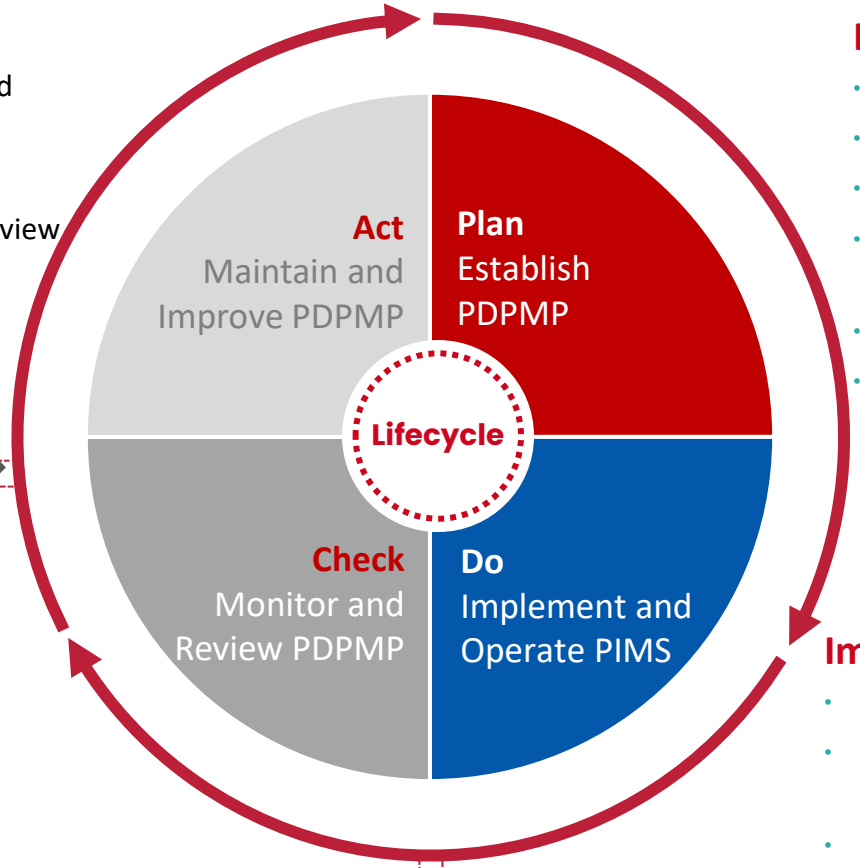
- Collect information security management requirements
- Define roles and responsibilities

External Drivers
- Laws & Regulations
- Market Environments
- Customer Expectations

Internal Drivers
- Business Needs
- Management Directions
- Contractual Obligations

Improve
- Remediation and Prevention
- Optimization
- Management review
- Roadmap for improvement

Requirements



Check
- Monitoring
- Audit
- Performance Measurement
- Analysis

Planning
- Objectives
- Strategy
- Organization
- Asset and risk identification
- KPI definition
- Schedule

Values

Implementation
- Release of Policies
- Training and Education
- SOPs

Outcome
- Requirements are aligned with security goals and business objectives
- Mature privacy management operation model

3

Experience sharing on how to cope with risks brought by technological developments

Some common risks associated with technological developments

- **Data Breaches and Cybersecurity Threats:** As technology advances, the risk of data breaches and cybersecurity threats increases. This includes unauthorized access to sensitive information, hacking, malware attacks, and phishing attempts
- **Privacy Concerns:** Technological developments often involve the collection, storage, and processing of personal data. This raises concerns about privacy, data protection, and compliance with privacy laws and regulations
- **System Failures and Downtime:** Technological systems may experience failures or downtime, leading to disruptions in operations, loss of productivity, and potential financial losses
- **Emerging Technologies and Uncertainty:** The adoption of emerging technologies, such as artificial intelligence (AI), blockchain, or Internet of Things (IoT), brings new risks and uncertainties. These technologies may have vulnerabilities or unintended consequences that organizations need to address
- **Third-Party Risks:** Engaging with third-party vendors, suppliers, or service providers for technological solutions introduces additional risks. These risks include data breaches, inadequate security measures, or non-compliance with privacy and security requirements
- **Ethical Considerations:** Technological developments raise ethical concerns, such as the responsible use of AI, automation's impact on jobs, and the potential for bias or discrimination in algorithms

Experience sharing on how to cope with risks brought by technological developments

- **Continuous Learning and Monitoring:** Stay updated with technological advancements and emerging risks by continuously learning and monitoring industry trends and developments
- **Risk Assessment and Management:** Conduct regular risk assessments to identify potential risks associated with technological developments
- **Collaboration with Stakeholders:** Working closely with IT teams, legal and business units to develop and implement appropriate measures
- **Regular Policy and Procedure Review:** Regularly review and update organizational policies and procedures to ensure they address risks associated with technological developments. This includes privacy policies, security measures, and data handling procedures
- **Monitoring and Auditing:** Establish monitoring and auditing mechanisms to regularly check the security of technology systems and data. Timely identification and resolution of potential issues, along with necessary corrections and improvements, are essential
- **External Expert Support:** Seek external expert support such as technical consultants, legal advisors, or security specialists. They can provide guidance on risk management and compliance, as well as help address specific technological risk concerns

DRIVEN to Win

Coca-Cola
SWIRE COCA-COLA