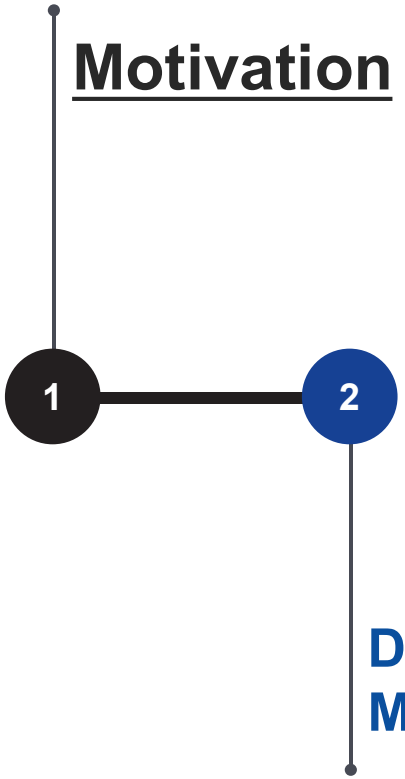

NANYANG
THE INNOVATIVE POLYTECHNIC

# Data Privacy and Protection

**Topic 5**

DPMP
Data Protection Management Programme

# Contents



# Data Protection Management Programme

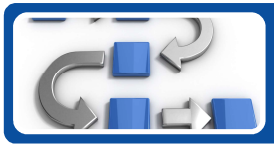
… builds a strong foundation for data protection within the organisation

1. 

Governance and Risk Assessment

2. 

Policy and Practices

3. 
Processes

4. 
Maintenance

# Data Protection Management Programme

… helps organisations to demonstrate accountability in data pr


**Stakeholders and Regulators**

**Business Competitiveness**

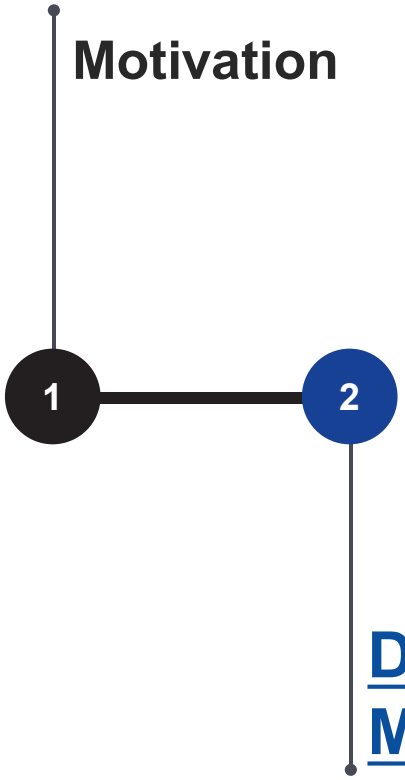

**Customers and Business Partners**

# Data Protection Management Programme

… helps organisations to demonstrate accountability in data protection


https://youtu.be/1vLsCUz8XSI

# Contents



# 1 Governance and Risk Assessment



**Governance Structure and Values**

**Risk Assessment**

# Role of Senior Management





To provide leadership through

1. Defining corporate values that are aligned with data protection
2. Allocating resources to data protection
3. Appointing a Data Protection Officer (DPO)
4. Managing personal data protection risks
5. Providing guidance on data protection initiatives
6. Supporting data protection policies and programme
7. Commissioning Data Protection Impact Assessments
8. Advocating data protection training
9. Providing directions to the DPO

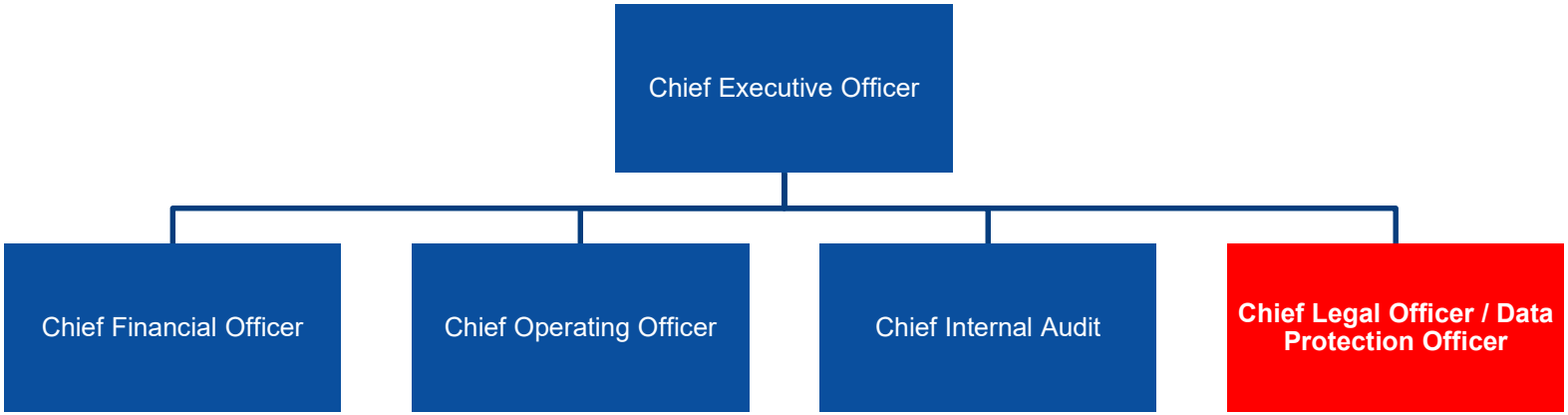
# Role of Data Protection Officer




It is mandatory for all companies in Singapore to appoint a Data Protection Officer

# DPO in an Organisation



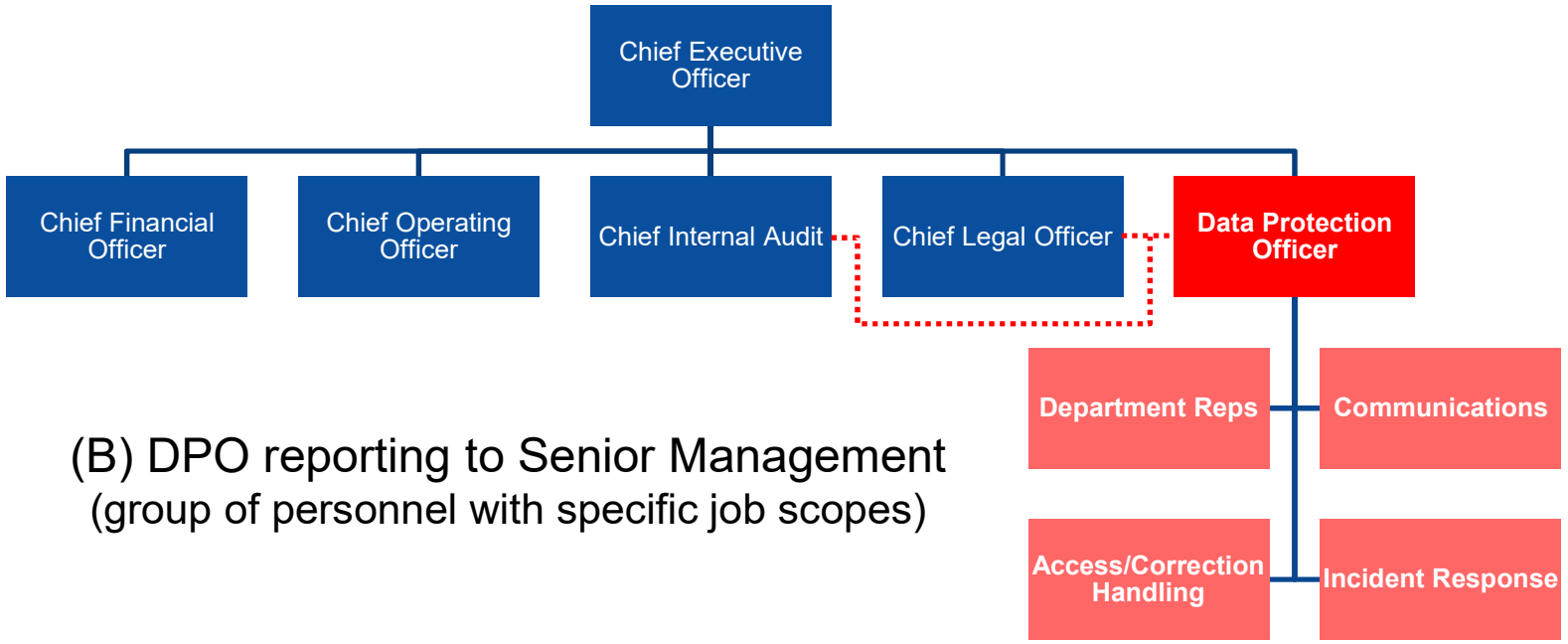




(A) Personnel within senior management appointed as the DPO

# DPO in an Organisation



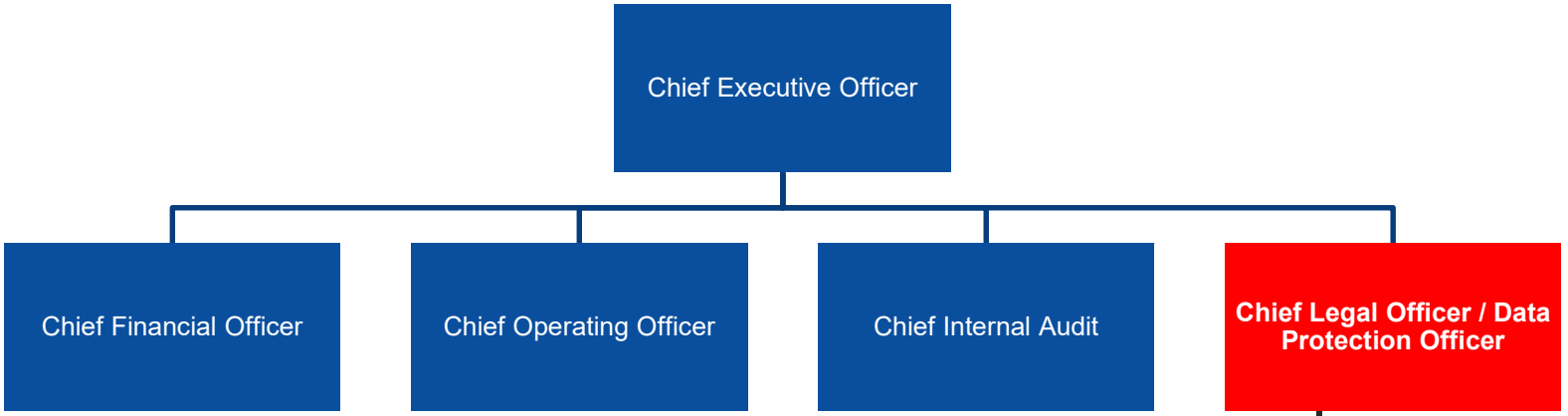





(B) DPO reporting to Senior Management
(group of personnel with specific job scopes)

# DPO in an Organisation




(C) The DPO operations may be outsourced to a service provider, however the DPO responsibility remains with a member of the senior management

Outsource

Data Protection-as-a-Service

# Culture of Accountability and Staff Training




Protecting personal data is the responsibility of everyone in the organisation – generate awareness and foster a culture of personal data protection

1. Personal data protection education for all staff, from Board to Senior Management to Staff
2. Trainings and briefings on personal data protection should be tailored to job functions
3. Regular staff communication circulars to include personal data protection topics

# Understanding and Identifying Risks





Senior management should have an understanding of risks and review how risks affects the organisation

**Strategic**

- Affects achieving company strategic objectives
- e.g. governance, strategic planning

**Operational**

- Affects organisational operations
- e.g. sales and marketing, production

**Compliance**

- Affects organisational compliance with regulations
- e.g. legal, code of conduct

**Financial**

- Affects organisational financial process
- e.g. reporting, tax

To manage risks, senior management should ensure that data protection is incorporated into their Risk Management framework

# 2 Policy and Practices



## Implementing Corporate Governance

Provides clarity. Demonstrates accountability.

# Data Privacy Policies




## Data Privacy Policies

- To comply to Personal Data Privacy regulations
- To set expectations for individuals

## Policies needs to explain:

- What data is collected
- Why the data is being collected
- What do you plan to do with the data
- Contact details for any questions or concerns

# Data Privacy Policies




## Policies needs to be understood:

- Use plain language
- Frequently Ask Questions
- Structured for the user
- Easily accessible

# An example:

**Data Protection Policy**

a) It is our responsibility to maintain the confidentiality of personal data and protect personal data against accidental or unlawful loss, unauthorised access, disclosure, copying, use or modification.

b) In our dealings with third parties e.g. outsourcing activities that require third party vendors to handle personal data of our staff or students, we must note that it is our responsibility to ensure that these third party vendors also provide the same level of data protection as NYP.

One way that we have done so is by including standard data protection clauses in the procurement contracts for such vendors to adhere to.

For details, pls refer to Staffassist -> Data Protection Policy -> Handling Enquiries on Personal Data

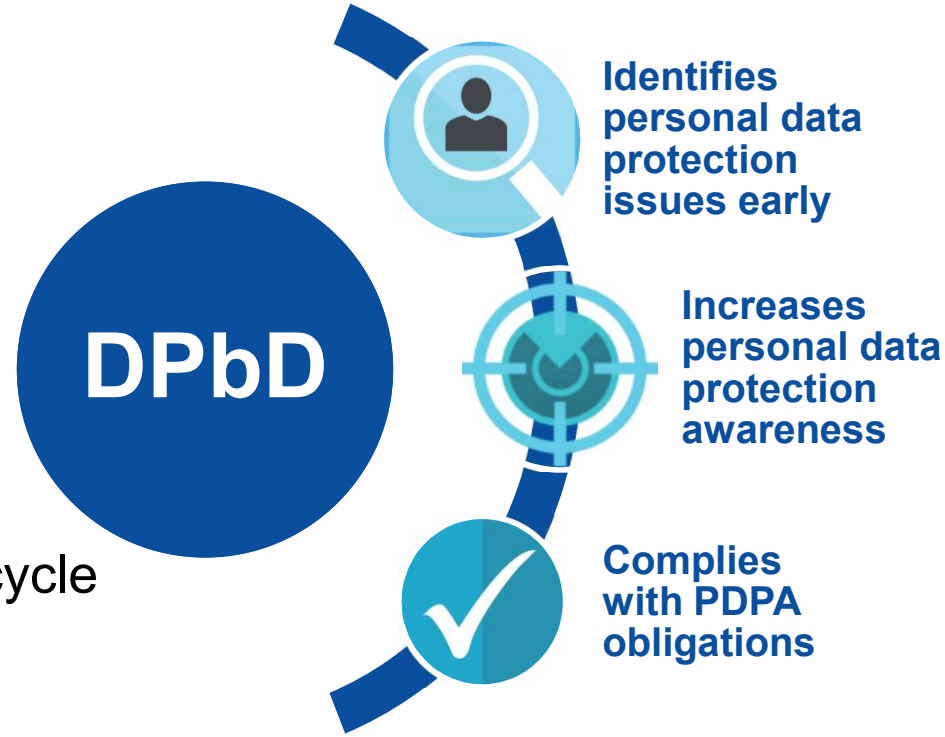
Ok

# Data Privacy Practices




## Data Protection by Design

Practicing personal data protection throughout the project's operational life cycle



# Key Elements of Data Protection by Design

Key elements of data protection by design include:

1. **Privacy by Default**: Systems should be configured to ensure that personal data is processed only as necessary for the intended purpose and that only necessary data is processed by default.
2. **Data Minimization**: It's essential to collect and process only the data that is necessary for the intended purpose. Avoiding the collection of excessive or irrelevant data is a key practice in data protection.
3. **Transparency and Accountability**: Implement measures to ensure transparency about data processing activities and to enable individuals to exercise their data protection rights. Additionally, ensure accountability for compliance with data protection laws and regulations.
4. **Security Measures**: Incorporate appropriate technical and organisational security measures to protect personal data against unauthorised access, disclosure, alteration, or destruction.
5. **Anonymization and Pseudonymisation**: Consider using techniques such as anonymisation or pseudonymisation to minimise the risks associated with processing personal data.
6. **User Empowerment**: Provide users with control over their personal data and enable them to make informed choices about how their data is collected, used, and shared.

# Data Privacy Communication




Organisations should ensure that personal data protection policies are communicated clearly and upfront


## Notification

- Publish policies and other information in simple language
- Use relevant channels (e.g. websites) that are easily accessible

## Consent

- Ensure that users understand what they are consenting
- simple and clear consent clauses at appropriate touchpoints

## Policy Updates

- Communicate any policy or service updates
- Communicate separately from other marketing messages

## Interaction with Users

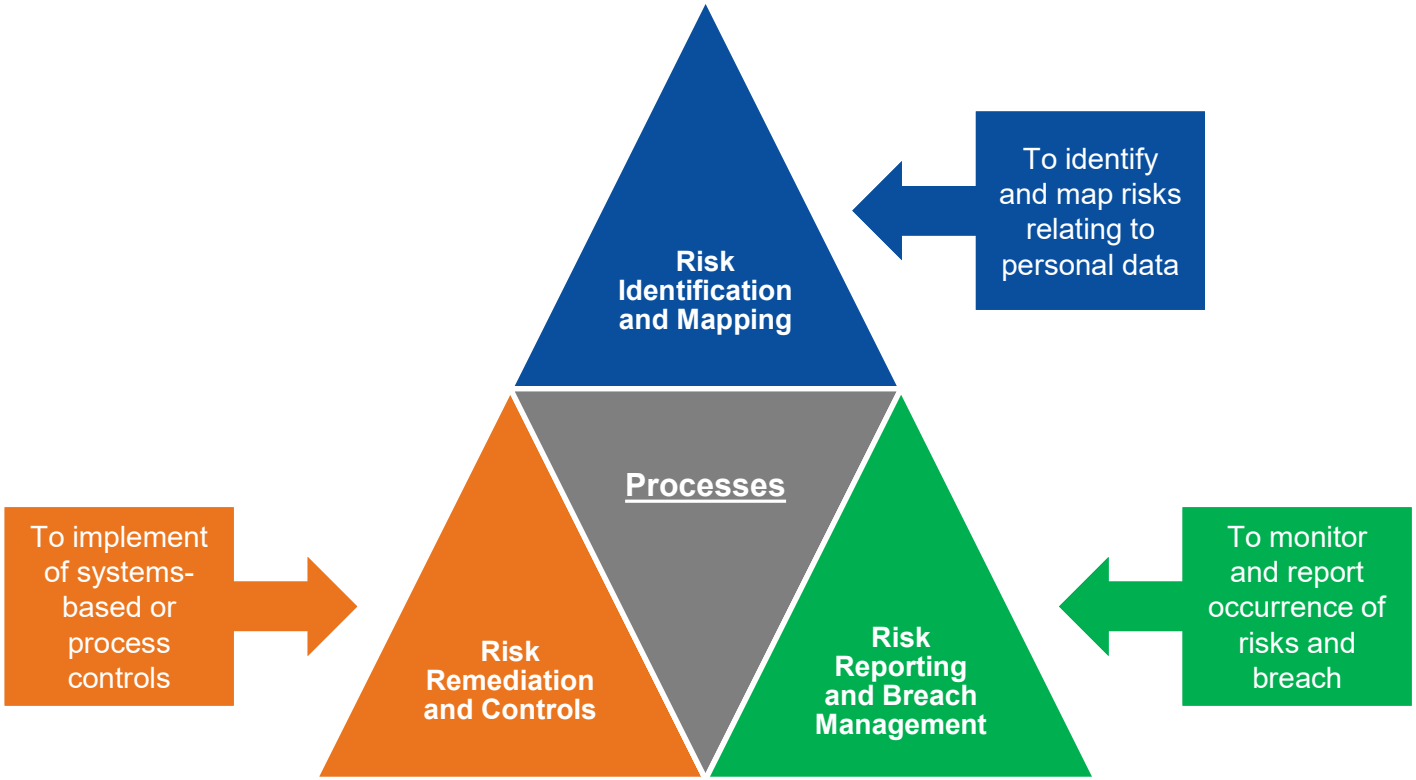
- Ensure staff interacting with users are trained in policy content
- Ensure staff sensitivity in handling data privacy feedback and queries

## Access, Correction, and Complaint Handling

- Provide accessible channels for users' requests
- Ensure proper processes and prompt response

# 3 Processes


1
2
3
Processes
4


Risk Identification and Mapping
To identify and map risks relating to personal data
Processes
To implement of systems-based or process controls
Risk Remediation and Controls
Risk Reporting and Breach Management
To monitor and report occurrence of risks and breach

# Risk Identification and Mapping





To identify and map risks relating to personal data, through using:

- Data Inventory Map – cataloguing personal data that includes, collection, use, disclosure, storage, disposal
- Data Flow Diagram – depicts the movement of that data through internal systems and external transfers
- Risk Register – records risks associated with the personal data and how it is used, likelihood and consequences of risk occurring

# Risk Identification and Mapping – Data Inventory Map

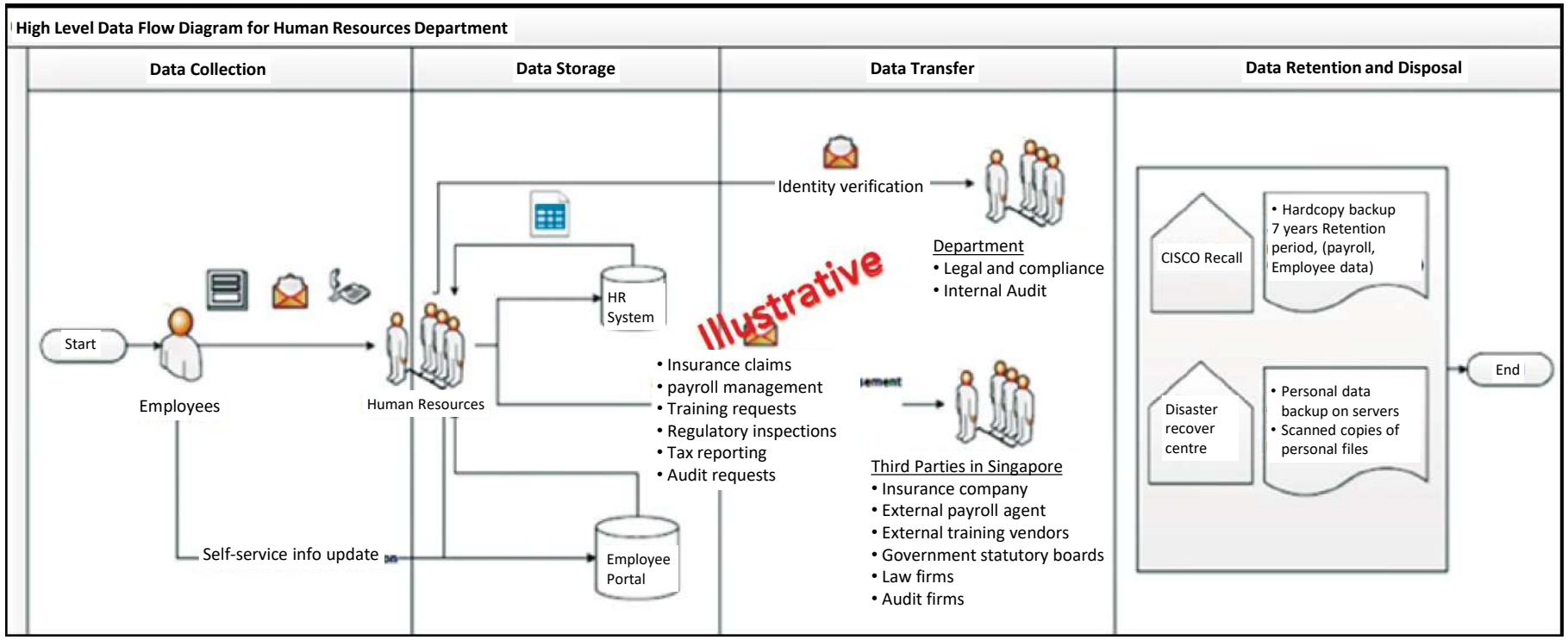



**Personal Data Inventory**

| No. | Department | Personal Data | Collection | | | | Use | | Disclosure to External Parties in Singapore | | Storage | | Transfer to External Parties outside Singapore | | Disposal &Archival | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Collection Purpose | Data Owner | Data Source | Collection Medium | Users of Personal Data and Purpose of Usage | Access to Personal Data | External Parties and Purpose of Transfer / Disclosure | Transfer Mode | Physical Storage | Electronic Storage | External Parties | Transfer Mode | Retention Period | Disposal Methods |
| 1 | Advertising and Marketing | Members:<br>- Name<br>- Email Address<br>- Contact Number<br>- Gender<br>- Nationality<br>- NRIC<br>- Membership | Market Research, Lucky Draw Contests, Send Newsletters and Promotions | Marketing | Customer Service | Hardcopy Forms, Emails, Softcopy | Database Team - Add data into databases | HR Compliance | Overseas marketing representatives<br><br>Research Agencies, Online Research Platforms<br><br>Starhub, M1, Singtel | NA | Hardcopy forms are in secured cabinets in secured rooms, accessible only via passes and keys | Databases | Overseas marketing representatives<br><br>Research Agencies, Online Research Platforms | NA | 1 year | Physical - Shredding<br>Electronic - Cleanup software |

# Risk Identification and Mapping – Data Flow Diagram



# Risk Identification and Mapping



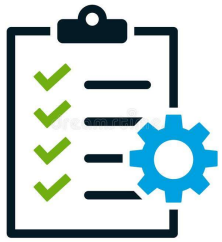


To identify and map risks relating to personal data, through using:

- Data Inventory Map – cataloguing personal data that includes, collection, use, disclosure, storage, disposal
- Data Flow Diagram – depicts the movement of that data through internal systems and external transfers
- Risk Register – records risks associated with the personal data and how it is used, likelihood and consequences of risk occurring

# Risk Remediation and Controls



**Risk management and remediation steps:**

1. Identify where personal data is stored
2. Determine level of security controls required
3. Apply controls on systems/infrastructure that stores personal data
4. Implement process controls to approve, review and manage access rights
5. Build data protection measures during the software development lifecycle

# Risk Reporting and Breach Management




To ensure that

- ongoing monitoring of personal data protection risks
- regular reporting of risks and incidents to senior management – quarterly or annually

To manage breach by

- **C**ontaining the breach
- **A**ssess the risk
- **R**eporting the incident
- **E**valuating appropriate response and recover procedures

# 4 Maintenance


# Reviewing Policies and Practices






Changes in environment may require revisions to data protection policies and processes.

Organisations will have to decide whether the reviews should be applied immediately or periodically

| Immediate (Ad-hoc) | Periodic |
|---|---|
| Major data leakage incident | Revision of data protection policies and processes at regular intervals |
| Legislative or regulatory amendments | Batch review of occurrences of minor incidents |
| Organisational changes | |

# Auditing




Organisations can conduct an audit to monitor and evaluate the overall implementation of the company's data protection policies and processes.

This could be done by

- An internal audit periodically
- An ad-hoc inspection or walk-through
- Obtaining and maintaining certifications for the organisation's data protection measures
- External audit

# Monitoring Changes




Organisations need to keep up to date with changes and developments within and outside the organisation.

Monitoring the environment could include

| External Environment | Internal Environment |
|---|---|
| Amendments to regulations | New or updated systems or processes |
| Data best practices or data incidents in other organisations | New business model |
| Technological changes or emerging technologies | Data incidents or feedback/complaints |

# Contents