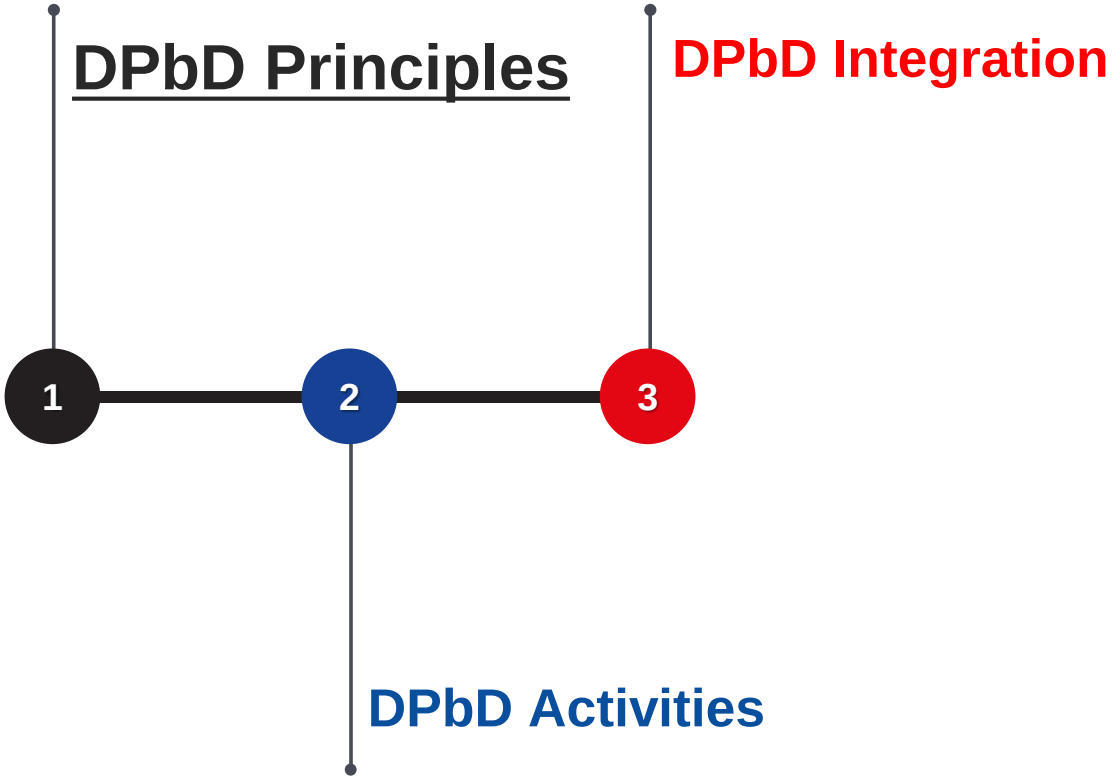

NANYANG
THE INNOVATIVE POLYTECHNIC

# Data Privacy and Protection

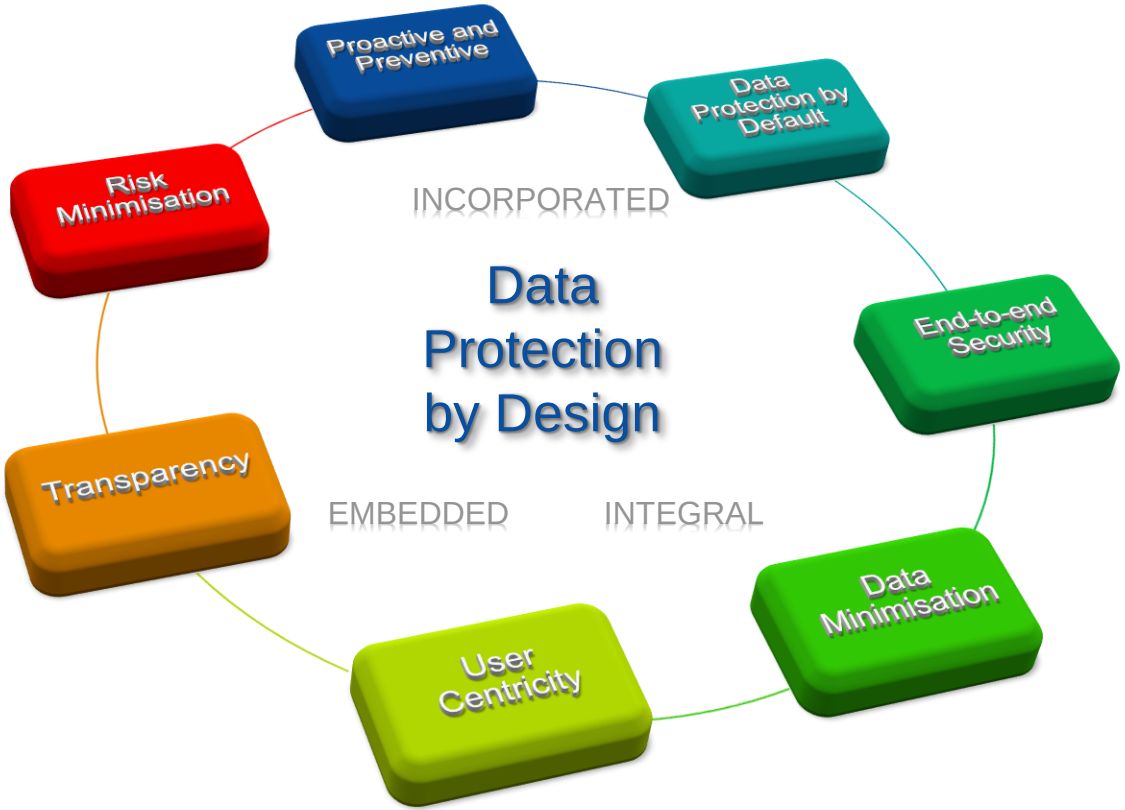
**Topic 7**

Data Protection by Design

# Contents



# Data Protection by Design



# DPbD Principles: Proactive and Preventive


DPbD approach is characterized by proactive rather than reactive measures

- It anticipates and prevents personal data invasive incidents
- It comes before-the-fact, not after.

DPbD begins with recognising the value of proactively adopting data protection practices

- Assess, identify, manage and prevent any data protection risks before data breaches occur
- Good design and data management practices.

# DPbD Principles: Data Protection by Default


DPbD ensures that personal data are automatically protected in any given system or process

- If an individual does nothing, their personal data is protected
- No action is required on the part of the individual.

Data protection measures must be

- Integrated into processes and features of the systems
- Automatically provided as default settings.

# DPbD Principles: End-to-end Security


Data protection measures must be embedded into the entire SDLC

- From the point that personal data is collected until it is purged from the system
- Applied security must assure the confidentiality, integrity and availability of personal data.

Personal data must be continuously protected across the entire domain and throughout the life-cycle of the data, including

- Across the entire business and 3rd party organisations
- Across the entire IT system eco-system.

# DPbD Principles: Data Minimisation


Data minimisation means to strictly collect, store and use personal data that is relevant and necessary

- Direct way to limit personal data leakage
- Do not “collect first and think of what to do with it later”.

Key actions include

- Assess for data minimisation throughout the data lifecycle – map data to specific purpose
- Create a Data Retention Schedule suitable that is the business.

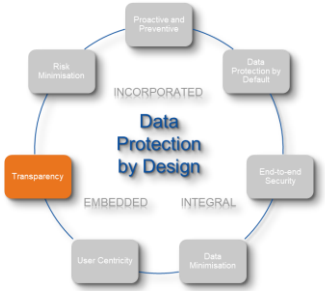
# DPbD Principles: User Centricity


Systems and processes should be developed with the interest of the individuals in mind.

Empowering individuals to play active role in managing their own data may be the single most effective check against abuse and misuse

- Consent – specific consent for the collection, use or disclosure of personal information
- Access – personal information is accurate and complete, provide access to review and have it amended.

# DPbD Principles: Transparency




Transparency and visibility are essential to establishing accountability and trust.

Key actions include

- Take an active role in informing individuals on what personal data is collected from them and how it is being used, as well as if there are any third parties involved in processing their personal data
- Identify and use appropriate means to provide such information

# DPbD Principles: Risk Minimisation

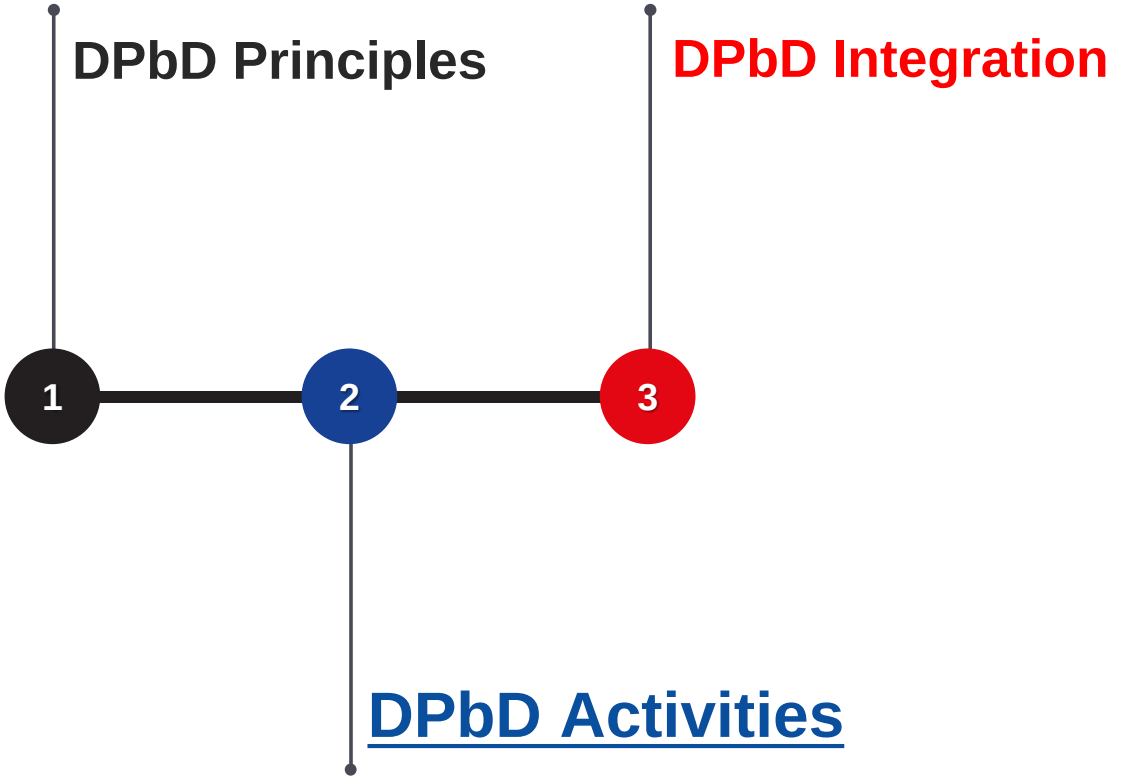

An important aspect of DPbD is,

- to prevent or reduce the likelihood of adverse incidents, or
- to reduce the impact of adverse incidents that do occur.

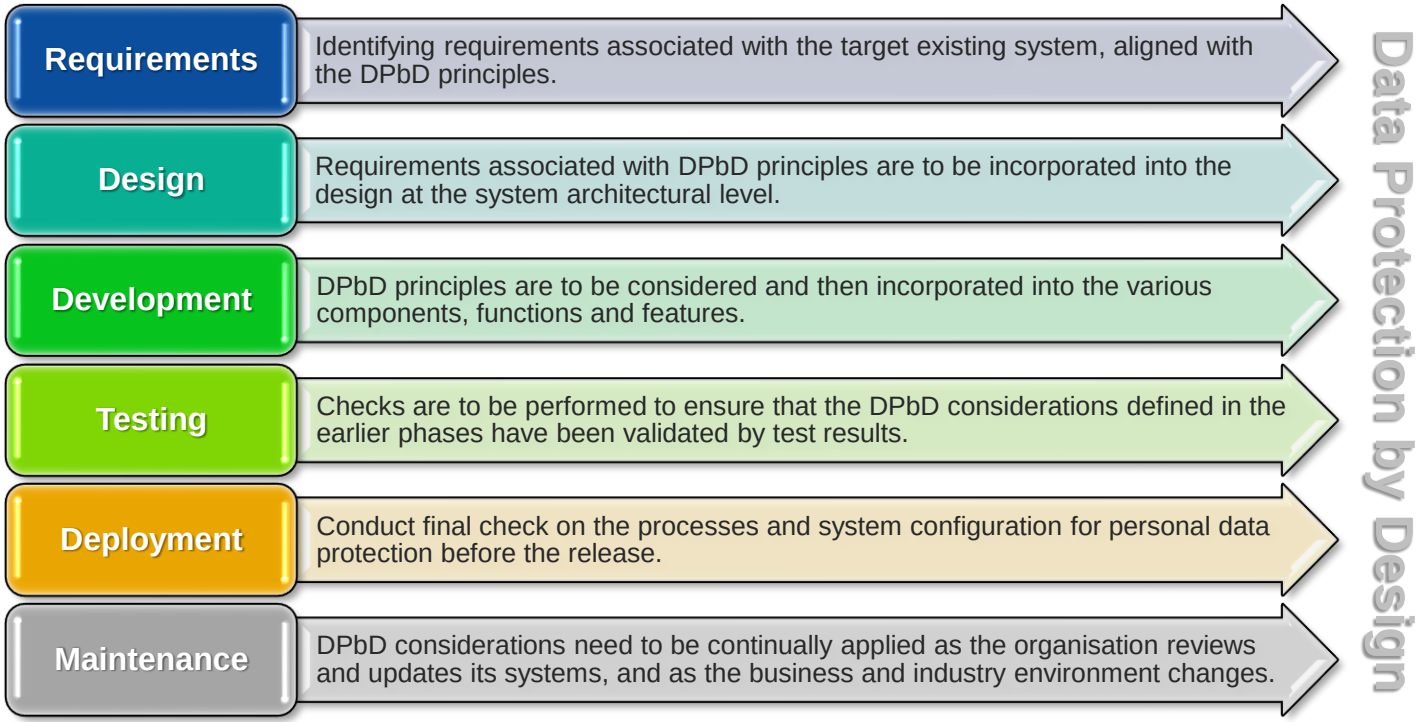
Key actions include

- Systematically identify and mitigate data protection risk, as much and as early as possible
- Designing and implementing the right processes and relevant data protection measures when processing personal data
- Monitor the effectiveness of risk minimisation measures

# Contents



# DPbD Activities in Systems Development Life Cycle



# DPbD Activities: Waterfall vs Agile Methodology

## Similarities

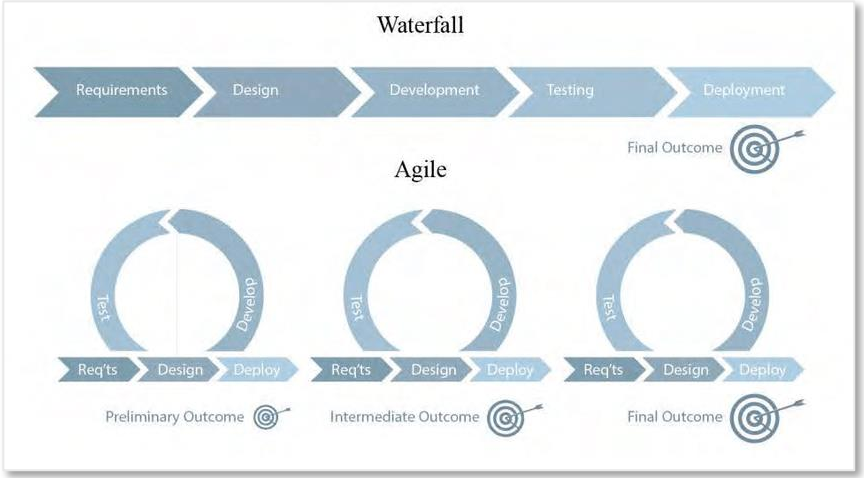
- Similar goals, which are to produce high-quality systems
- Same activities, from collecting requirements, to designing, developing, testing, and deploying

## Difference

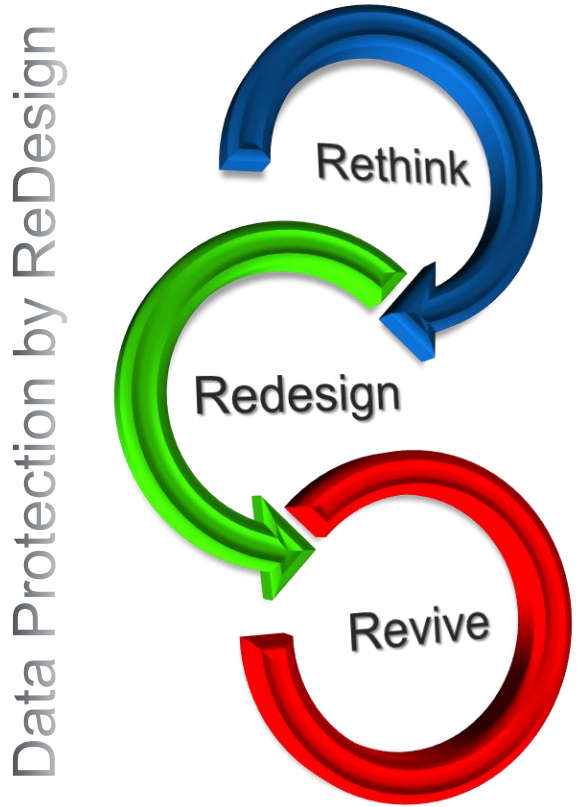
- Waterfall is a linear approach and divides a project into phases
- Agile is an iterative approach that separates a project into sprints

## DPbD activities

- Applicable to both development models
- More flexibility and less cost to design and implement DPbD features from earlier stages



# DPbD Activities: Existing Systems




## Rethink

- Identify business and personal data protection requirements against existing system business
- Evaluate existing system privacy controls against DPbD Principles

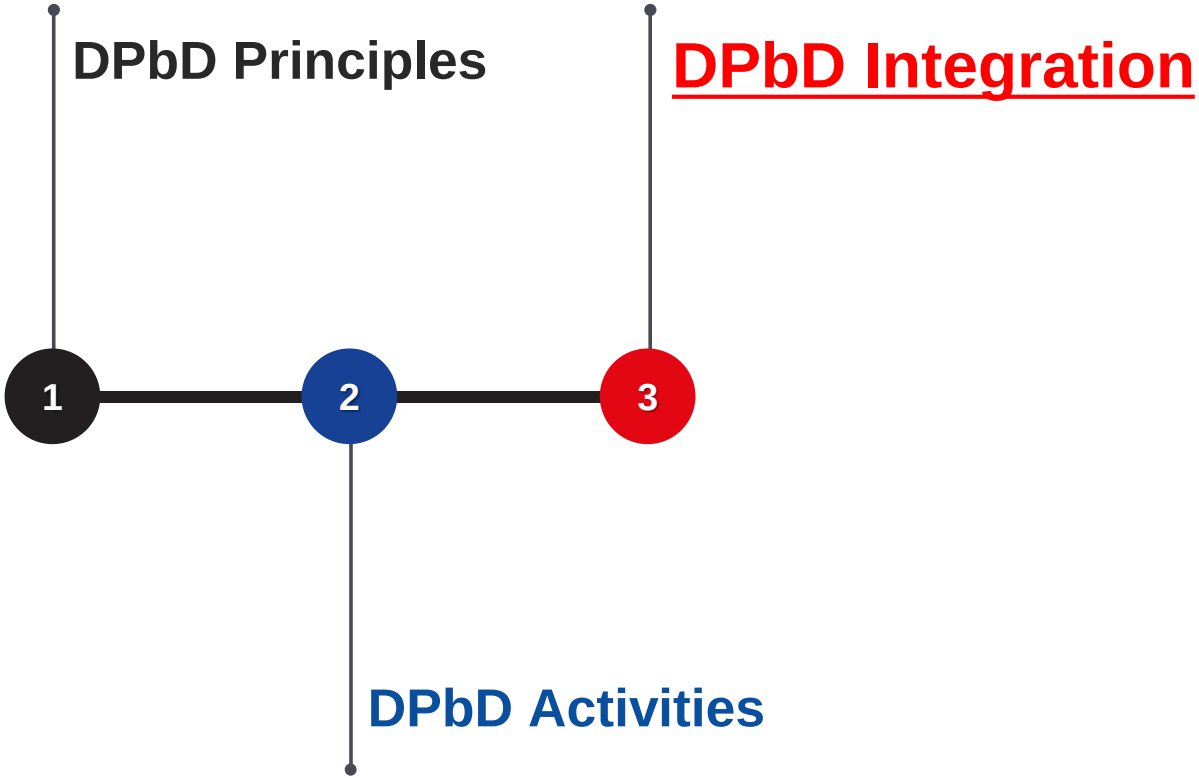
## Redesign

- Design and develop relevant DPbD controls to meet personal data protection requirements
- Reduce the risks identified during the “Rethink” stage

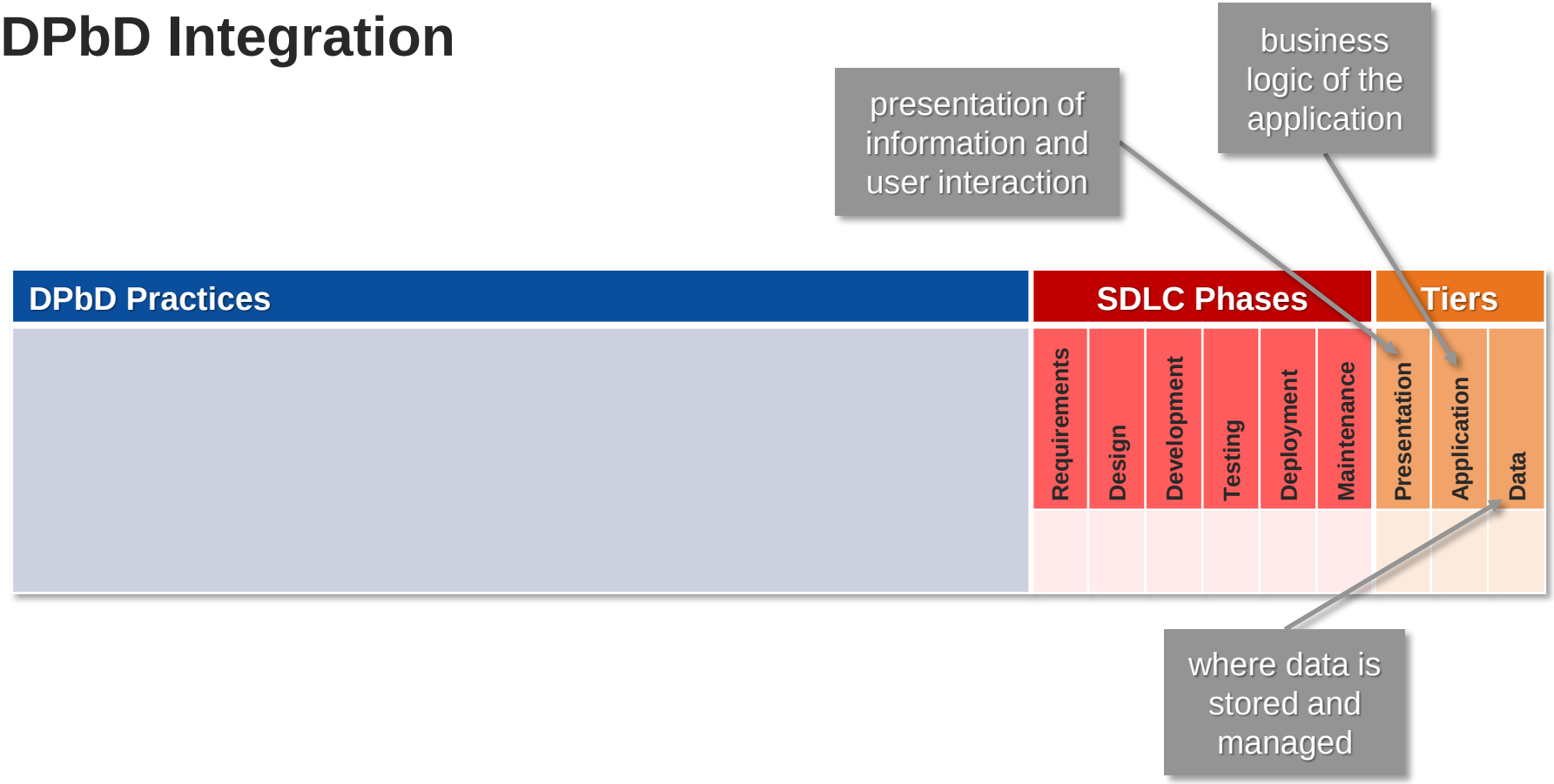
## Revive

- Revalidate and implement the redesigned, personal data protection-enhanced system
- Confirm successful integration of redesigned target system

# Contents



# DPbD Integration



# DPbD Integration: DPIA

DPIAs may be conducted at any point in time during the SDLC, however a good time to conduct them is when the preliminary design of a new system has been established.

| DPbD Practices | SDLC Phases | | | | | | Tiers | | |
|---|---|---|---|---|---|---|---|---|---|
| | Requirements | Design | Development | Testing | Deployment | Maintenance | Presentation | Application | Data |
| **1. Conduct DPIA before development**<br>Assess the types of personal data and the data processing activities required for achieving the purposes of the new system. This helps to identify and assess for any risks in the design of the new system. The design of the system may then be modified and mitigating measures may be incorporated, if necessary. | ✓ | ✓ | | | | ✓ | | | |

# DPbD Integration: Purpose Limitation

Collect personal data that the organisation really needs. Personal data that is collected but not used, only burdens organisations with unnecessary risks.

| DPbD Practices | SDLC Phases | | | | | | Tiers | | |
|---|---|---|---|---|---|---|---|---|---|
| | Requirements | Design | Development | Testing | Deployment | Maintenance | Presentation | Application | Data |
| **1. Minimise collection of personal data**<br>Do not collect personal data unless it will be used, and there is a valid purpose for doing it. Collect the least sensitive types of personal data. | | | | | | | | | |
| **2. Collect information on personal identifiers only when it is absolutely necessary**<br>These tend to be unique values that directly identify persons. Hence, extra consideration should be given as to whether there is a need to collect. | ✓ | ✓ | | | | ✓ | ✓ | ✓ | |
| **3. Collect personal data through user input instead of automatically or continually or obtaining**<br>Some users may prefer convenience, but others may prefer less intrusion and prefer to provide input when it is needed. | | | | | | | | | |

# DPbD Integration: Notification

Organisations are required to notify individuals of the purposes and obtain their consent for collecting, using and disclosing their personal data.

| DPbD Practices | SDLC Phases | | | | | | Tiers | | |
|---|---|---|---|---|---|---|---|---|---|
| | Requirements | Design | Development | Testing | Deployment | Maintenance | Presentation | Application | Data |
| **1. List personal data collected and explain the purpose of collection**<br>This means the 'what', 'how', and 'why' related to personal data collected. This applies especially when it may not be obvious to the user why certain information about them is being collected. | | ✓ | ✓ | | | ✓ | ✓ | | |
| **2. Keep it simple**<br>Keep the organisation's data protection policy statement concise and readable. | | | | | | | | | |
| **3. List third parties**<br>List out third parties involved in processing the personal data (if any), what personal data is passed to the third parties. | | | | | | | | | |

# DPbD Integration: Notification (… continued)

Organisations are required to notify individuals of the purposes and obtain their consent for collecting, using and disclosing their personal data.

| DPbD Practices | SDLC Phases | | | | | | Tiers | | |
|---|---|---|---|---|---|---|---|---|---|
| | Requirements | Design | Development | Testing | Deployment | Maintenance | Presentation | Application | Data |
| **4. Layered approach**<br>Present an overview first and allowing the user to choose which sections to view in greater detail. | ✓ | ✓ | ✓ | | | ✓ | ✓ | | |
| **5. Just-in-time approach**<br>A “just-in-time” or dynamic approach is to notify just before certain personal data is collected or certain permission is required. | | | | | | | | | |

# DPbD Integration: Consent

Getting users' consent to use their personal data is something that IT systems can help achieve very effectively.

| DPbD Practices | SDLC Phases | | | | | | Tiers | | |
|---|---|---|---|---|---|---|---|---|---|
| | Requirements | Design | Development | Testing | Deployment | Maintenance | Presentation | Application | Data |
| **1. Require explicit action for the user to indicate consent**<br>Ensure that user has to perform an explicit action to indicate consent. | | ✓ | ✓ | | | ✓ | ✓ | | |
| **2. Ask separately for consent to receive marketing materials**<br>For marketing, ask separately for the consent to collect personal data, e.g. via a second checkbox. | | | | | | | | | |

# DPbD Integration: Consent (… continued)

Getting users' consent to use their personal data is something that IT systems can help achieve very effectively.

| DPbD Practices | SDLC Phases | | | | | | Tiers | | |
|---|---|---|---|---|---|---|---|---|---|
| | Requirements | Design | Development | Testing | Deployment | Maintenance | Presentation | Application | Data |
| **3. Keep records of what users consented**<br>Users may consent to certain elements but not others. Therefore, it is important to keep records of what users have consented to and when these were obtained. | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ | |
| **4. Allow users to withdraw their consent**<br>This could be implemented through a manual process, or using a more automated way. It is useful to inform users of the consequences of withdrawing their consent (if any). | | | | | | | | | |

# DPbD Integration: Accuracy, and Access & Correction

Organizations should ensure that the personal data collected is accurate, and individuals have the right to request for access to their personal data and for correction of their personal data.

| DPbD Practices | SDLC Phases | | | | | | Tiers | | |
|---|---|---|---|---|---|---|---|---|---|
| | Requirements | Design | Development | Testing | Deployment | Maintenance | Presentation | Application | Data |
| **1. Provide users with a self-management facility**<br>Allow users to manage their personal data without requiring employee assistance. | | | | | | | | | |
| **2. Ensuring that user updates are done**<br>Periodically remind users to use the self-management, or making sure users view their details and acknowledge that they are correct. | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ | |

# DPbD Integration: Protection

Organizations should ensure that the personal data collected is accurate, and individuals have the right to request for access to their personal data and for correction of their personal data.

| DPbD Practices | SDLC Phases | | | | | | Tiers | | |
|---|---|---|---|---|---|---|---|---|---|
| | Requirements | Design | Development | Testing | Deployment | Maintenance | Presentation | Application | Data |
| **1. Implement measures against the OWASP Top 10 Most Critical Web Application Security Risks**<br>This list explains the most common and critical security risks in web applications. | | | | | | | | | |
| **2. Encrypt data at rest**<br>Encrypt personal data to provide additional security. Review the method of encryption periodically to ensure that it is recognised by the industry as relevant and secure. | ✓ | ✓ | ✓ | ✓ | | ✓ | | ✓ | ✓ |
| **3. Implement access control**<br>Access control is a fundamental way to protect personal data. It often refers to authentication and authorisation. | | | | | | | | | |

# DPbD Integration: Retention Limitation

Housekeeping of personal data in IT systems.

| DPbD Practices | SDLC Phases | | | | | | Tiers | | |
|---|---|---|---|---|---|---|---|---|---|
| | Requirements | Design | Development | Testing | Deployment | Maintenance | Presentation | Application | Data |
| **1. Manage expired personal data properly**<br>These records should be deleted or anonymised. | | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ |
| **2. Avoid letting temporary files containing personal data become permanent**<br>Temporary files could be generated, e.g., an intermediate form for interfacing with other systems. Protect such temporary files while they exist, and remove them once they are not required. | | | | | | | | | |
| **3. Be careful with data migration files**<br>There is also the danger of the data migration phase dragging on. This can result in data migration files being forgotten, leading to permanent vulnerability. | | | | | | | | | |

# DPbD Integration: Accountability

After the system has gone live, it is typical for the technical team to be scaled down in terms of manpower. However, the organisation continues to be Accountable to provide care for the personal data.

| DPbD Practices | SDLC Phases | | | | | | Tiers | | |
|---|---|---|---|---|---|---|---|---|---|
| | Requirements | Design | Development | Testing | Deployment | Maintenance | Presentation | Application | Data |
| **1. Watch out for updated legal requirements or technology changes**<br>Laws change over time. Similarly, technology changes may require tweaks to be made in the system design or implementation. | | | | | | ✓ | ✓ | ✓ | ✓ |
| **2. Keep data inventory updated**<br>Update the personal data inventory when changes are made to the system. | | | | | | | | | |
| **3. Continue to run security tests periodically**<br>Security testing should not end when the system goes live. | | | | | | | | | |

# Contents