



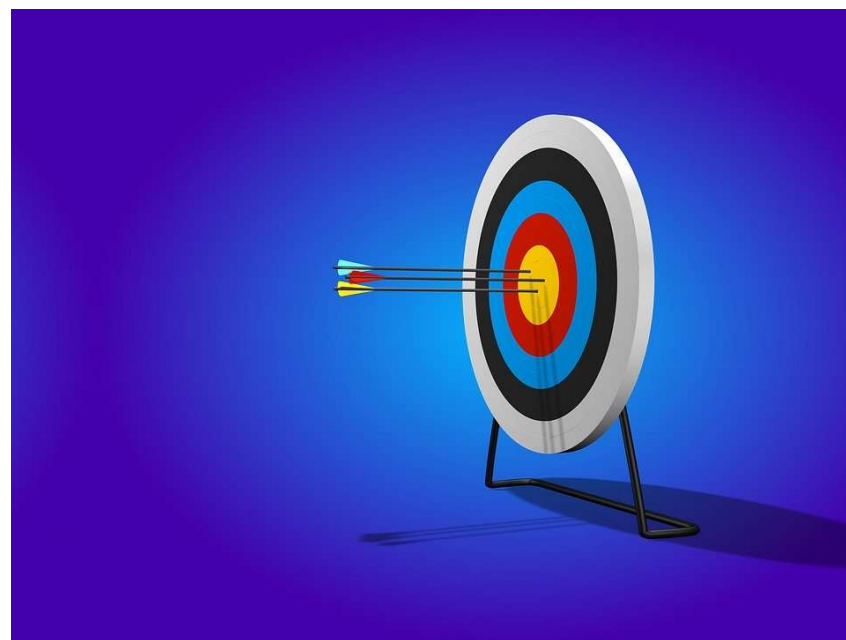
Personal Data Protection (PDP) Training

LTCs (Long Term Contractors)

© These slides contain confidential and proprietary information belonging to Resorts World at Sentosa Pte Ltd ("RWS") and are intended solely for internal use.
Unless permitted by DPO, these slides may not be reproduced, distributed to any non-RWS party and/or viewed by any non-RWS party, whether in whole or in part.

Learning Objectives

- Understand PDPA obligations
- Apply personal data responsibilities in your daily work



Types of Personal Data

Any data that identifies you is personal data

	1. DIRECT /Unique Identifiers	2. INDIRECT Identifiers – set of data <u>put together</u> would identify a person
Examples	• Name • Mobile phone number • National ID/ Passport number • Personal images • Biometric data (face recognition / thumbprint) • Other customer due diligence (CDD) information	• Age • Date of Birth • Gender • Address • Nationality Online profile containing the following information: • Mobile advertising identification numbers • IP addresses • Cookies

Personal Data that is **SENSITIVE**

Sensitive personal data **can cause great harm to individuals**

Sensitive personal data **CANNOT** be freely collected, used or disclosed without **strong legal basis**

Examples

- National identity data (**NRIC, passport**)
- **Sensitive Individuals**
Politically-Exposed-Person (PEP), Socialites, Patrons, Children's or vulnerable individuals
- **Financial data**
bank, loan and credit card details, salary, credit history, KYC and PMLTFPF data
- Race and ethnic origin,
and religious beliefs
- Criminal offence data
- Genetic or biometric data
- Health or medical data
- Images & voice recordings



Importance of Personal Data Protection



Purpose of PDP

- Safeguard personal data from misuse & maintain customer' trust in organisations



Regulatory Compliance

- RWS is legally responsible to protect the personal data of our guests to comply with PDPA
- Failure to comply can lead to fines and embarrassment for RWS



Competitive Advantage

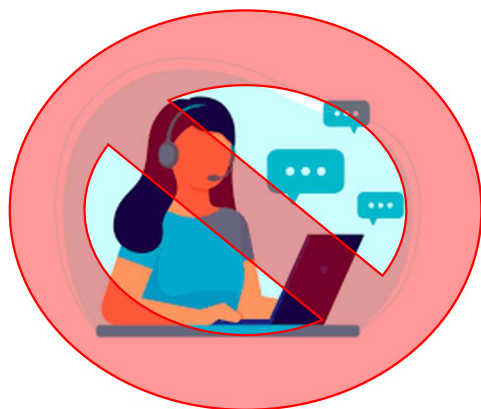
- A strong “personal data protection” culture strengthens RWS business reputation with higher guests' confidence and trust in our services
- **Data breach by one Business Unit (BU) will damage the reputation of whole organisation.**



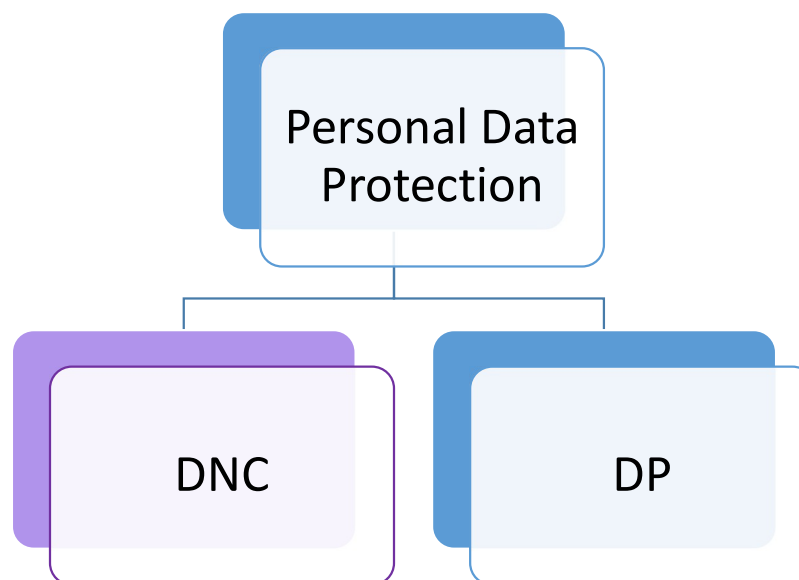
Personal Data Protection (PDP) Overview

PDPA contains **2** main sets of provisions

- i. Do Not Call (DNC) Provisions
- ii. Data Protection (DP) Provisions



- Marketing Message
- Telemarketing



DP Provisions contain **10 main obligations** to comply during collection, use or disclosure of personal data

Do Not Call (“DNC”) Registry & Spam Control

For Singapore telephone numbers that are registered with DNC Registry, **marketing messages are NOT allowed to be sent unless:**

- Clear and unambiguous consent has been obtained from guest to send marketing messages either via call, text or fax

When sending marketing messages :

Ensure consent is collected before sending

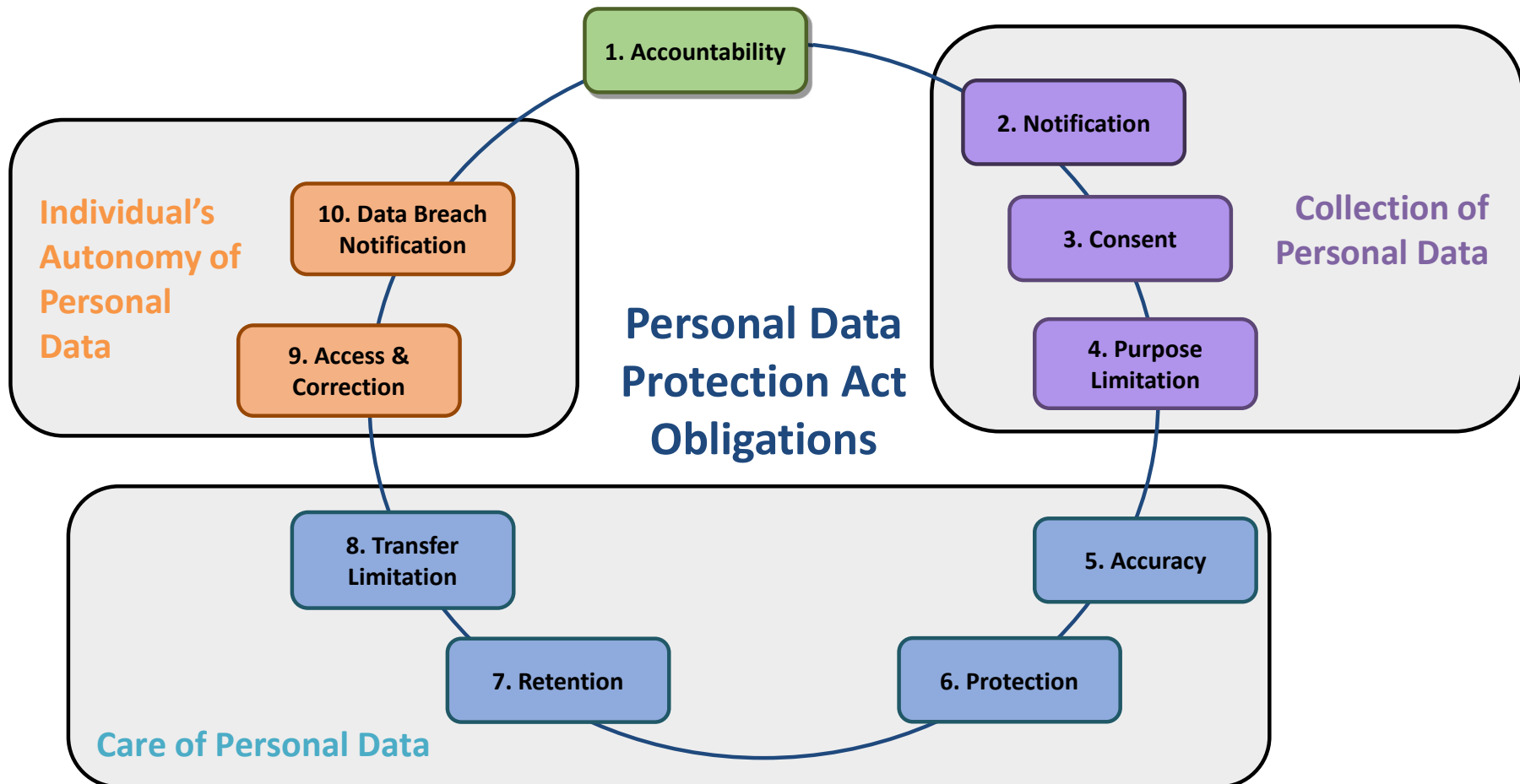
- ☑ Ensure message contains clear and accurate information
- ☑ Ensure an accurate and functional telephone number is used
- ☑ Ensure labelling of <ADV> before message and offer “unsubscribe” option if it is an advertising / marketing message

When making a phone call:

Ensure caller ID is displayed and not blocked



Data Protection (“DP”) - 10 Obligations

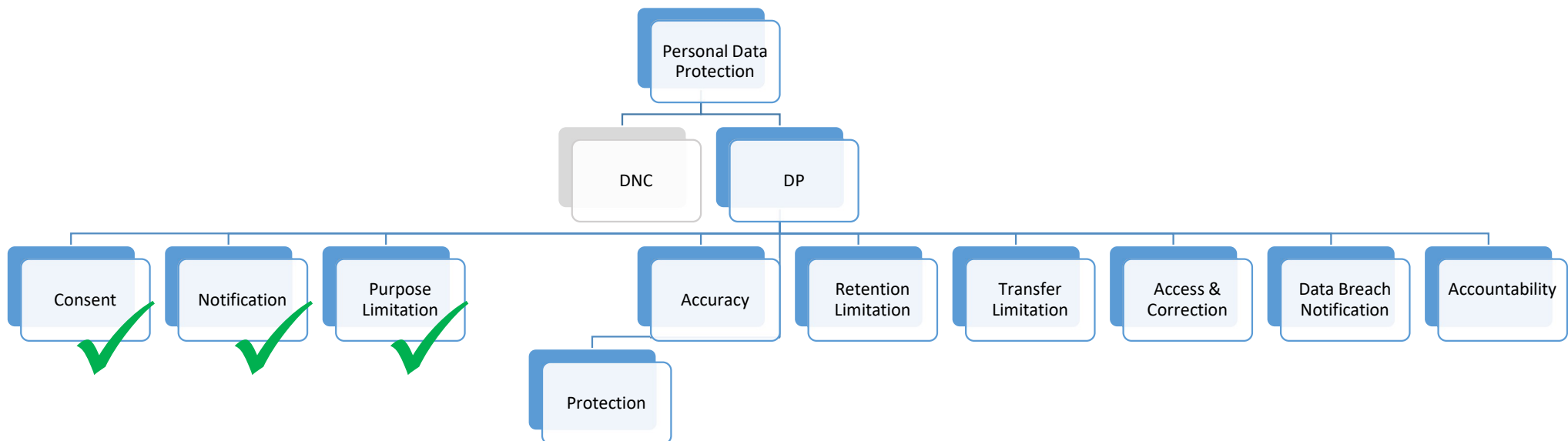




DP Obligations



DP Obligations to Consider during Collection



Collection of Consent

Valid consent is...

- *Voluntary*
- *Informed*
- *Reasonable (legitimate)*



Always consult the DPO on the appropriate approach to managing consent whenever a BU needs to collect personal data.

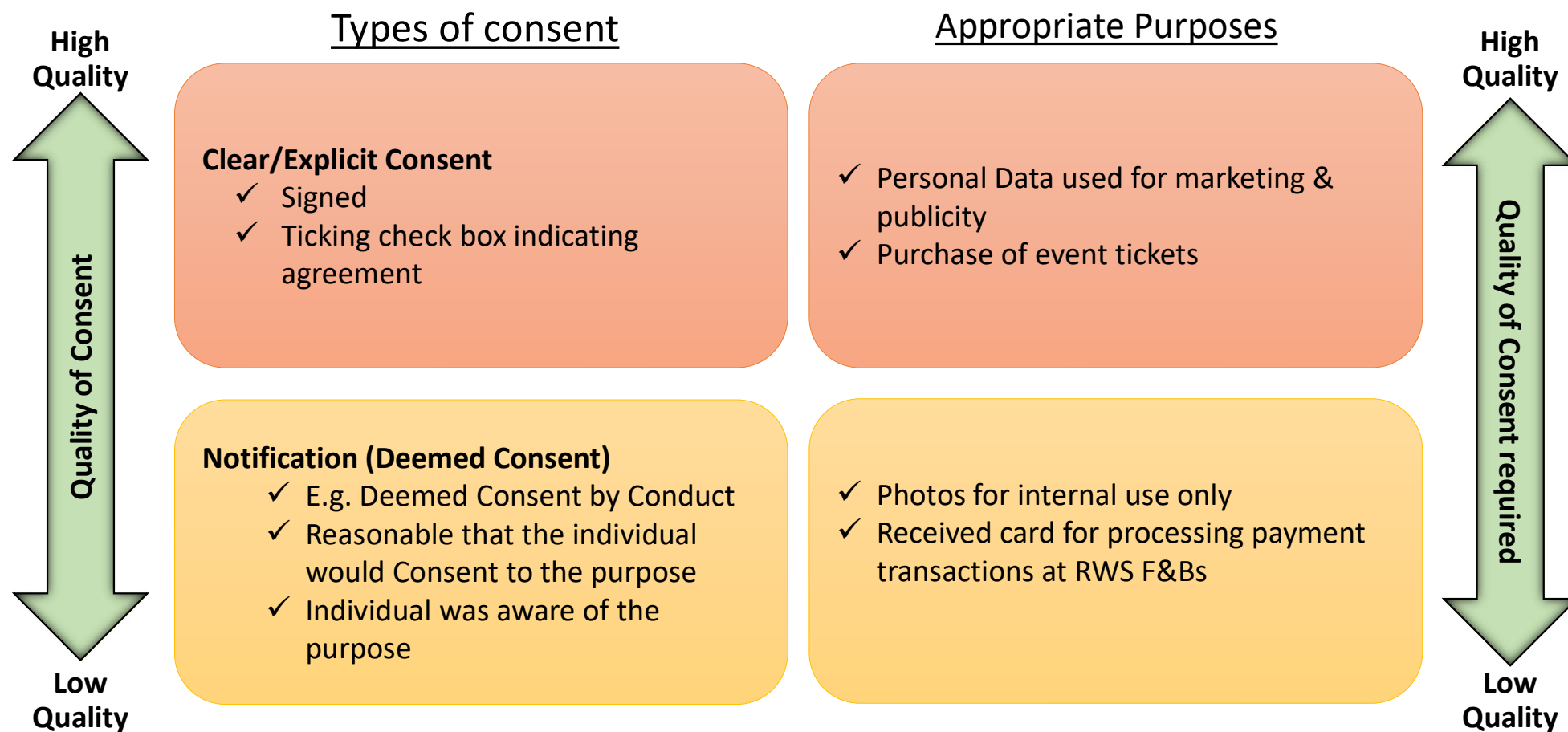
For example,

- *Introduce or redesign new process*
- *Launching new product, services or system*



Never obtain or attempt to obtain consent by providing false or misleading information or using deceptive or misleading practices

Consent vs Purpose



Purpose Limitation Obligation

Purpose Limitation

Always ensure a valid (reasonable) business purpose and legal basis when collecting personal data.

Example		Explanation
Valid Basis 	Collecting patron NRIC before allowing guest to check in to rooms	Collecting NRIC is necessary and a requirement under Hotels Licensing Regulations
Invalid Basis 	Collecting guest NRIC for entry into restaurants	NRIC is sensitive data and should not be freely collected without a strong or legal basis



Do not reuse collected personal data for other purposes where they were not consented to



Do not adopt “Collect first and think of what to do with it later” or “Just in case” approach

Notification Obligation

Notification

Always notify customer the purposes on why RWS intend to collect, use or disclose their personal data

Example		Explanation
Valid Basis 	"Your personal data will be used by RWS for analysis of survey responses and to improve customer experience at our resort"	Terms and conditions are clearly and legibly stated and notified at the beginning of survey form
Invalid Basis 	"Your personal data provided may be used and disclosed for any valid business purposes"	The stated notification is too general and not specific

Example of CCTV Notification Signage



DO NOT adopt "Collect first and think of what to do with it later" or "Just in case" approach

DP Obligations to Consider during Processing



Collect



Processing



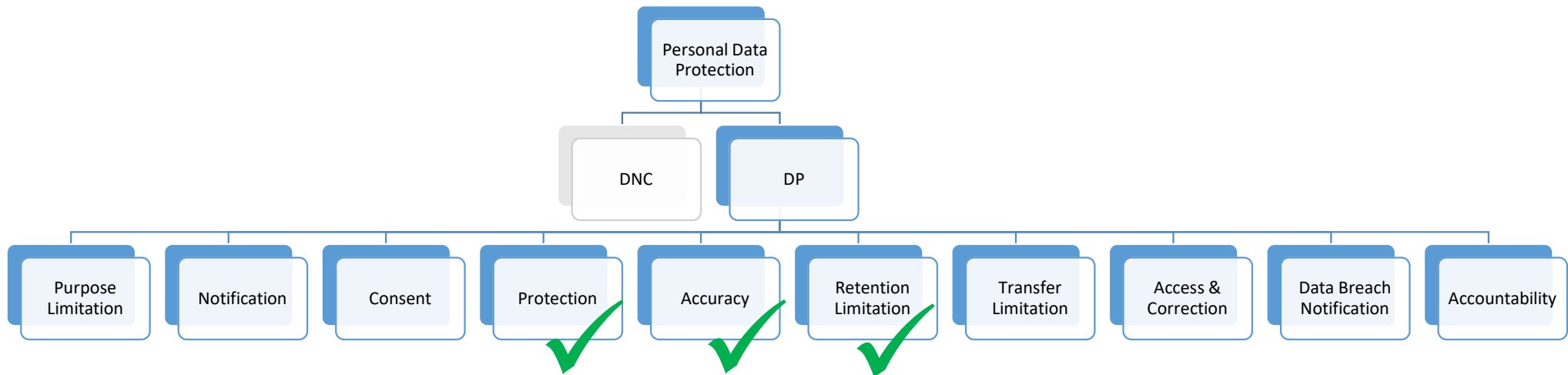
Store



Disclose



Dispose
销毁



Protection Obligation

After collection of personal data, all subsequent processing, storage & disclosure may involve personal data risks

- Unauthorized Access
- Unauthorized Processing
- Insecure Storage
- Unauthorized Copying
- Unauthorized Disclosure
- Insecure Disposal
- Others ...

These risks may have severe consequences of data breaches that will damage the reputation of the entire resort

Ensure Personal Data is Secured and Protected

Just like any RWS trade secrets and confidential information, Personal Data should also be kept secured and accessible only by authorized personnel to mitigate personal data risks

Examples of Basic Data Protection

- ☑ Ensure clear desk policy
- ☑ Ensure proper data classification
- ☑ Ensure data backup
- ☑ Ensure data encryption
- ☑ Ensure secure destruction



It is extremely **important** to handle the personal data with care

Protection Obligation

Examples of data protection controls :

Organizational Controls

- Contracts
- RWS policies
- Business unit (BU) SOPs
- Training

Technological Controls

- Encryption
- Passwords
- Access controls
- Secured computer systems

Physical Controls

- Locking the door / cabinet
- Shredding paper records
- Clear desk / Clear screen
- Recipient verification

Contractual Protections

- Check with RWS Legal for the proper controls to put in place before sharing any personal data

Check in with Subject matter experts

- Contact IT for advice on ensuring that personal data is properly secured before it is sent

Organizational Protections

- Periodically check that the data recipient is protecting the personal data

**PLEASE
HANDLE WITH CARE**

Accuracy Obligation

Prior to use or processing,

- Ensure that personal data is accurate
- Ensure all personal data is complete
- Ensure personal data is kept up to date



Do not assume data is accurate without verification



Do not use outdated personal data for processing



Do not collect data from unreliable sources

Retention Limitation Obligation

Personal data should only be retained if we have valid business or legal purpose for retaining the data

Example		Explanation
Valid Basis	Retaining personal data of active resort member	Active membership - clear ongoing legal and business purpose to retain the member's personal data
		
Invalid Basis	Retaining personal data "just-in-case", we might need it in the future	We should not retain personal data if we do not have a clear purpose for retaining the data
		

Collected personal data has to be securely disposed when it is not longer necessary or required for any legal or business purposes

Example		Explanation
Valid Basis	Securely disposing transaction records after 5 years	Finance require such transaction records to be retained for 5 years to comply with MAS regulations
		
Invalid Basis	Disposing personal data before the retention period has expired	If the retention period has not expired then we might be required to retain the personal data for legal or business purpose
		

Retention Limitation Good Practices

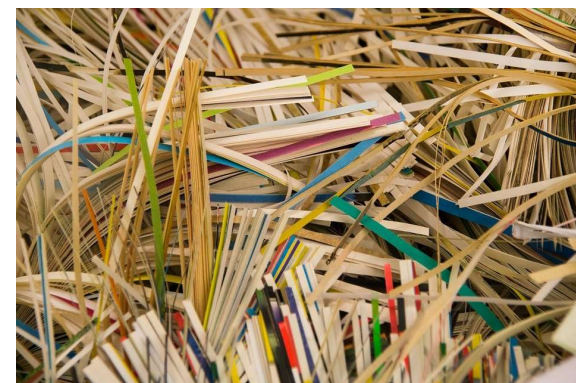
Retention principle

- Ensure compliance with the retention period as specified in the BU SOP).

Secure Destruction

- Destroy personal data securely e.g by using a company shredder or contact IT for advice
- Never throw it directly in the trash bin. Consider shredding instead

“Refer to Data Retention & Disposal Policy to find out more”



DP Obligations to Consider during transfer



Collect



Processing



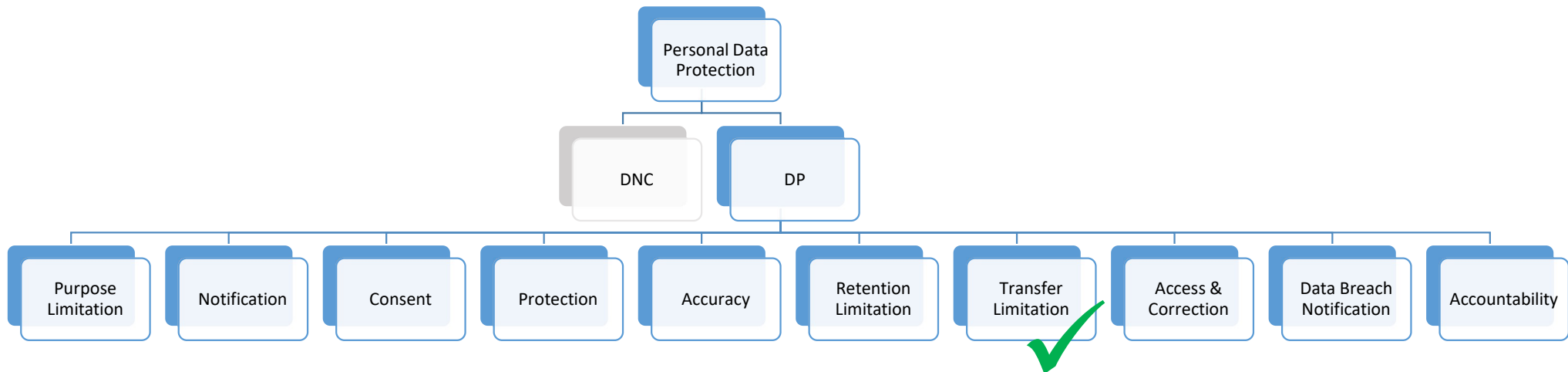
Store



Disclose



Dispose



Transfer Obligation

For personal data transferred out of Singapore

- Ensure data transferred is protected to the same standard as PDPA or higher
- Ensure contract with 3rd party has necessary data protection clauses and 3rd party must not further transfer data before obtaining approval from RWS
- Ensure customer has been notified and given valid consent

BU shall always consult DPO before conducting activities involving cross border personal data transfer



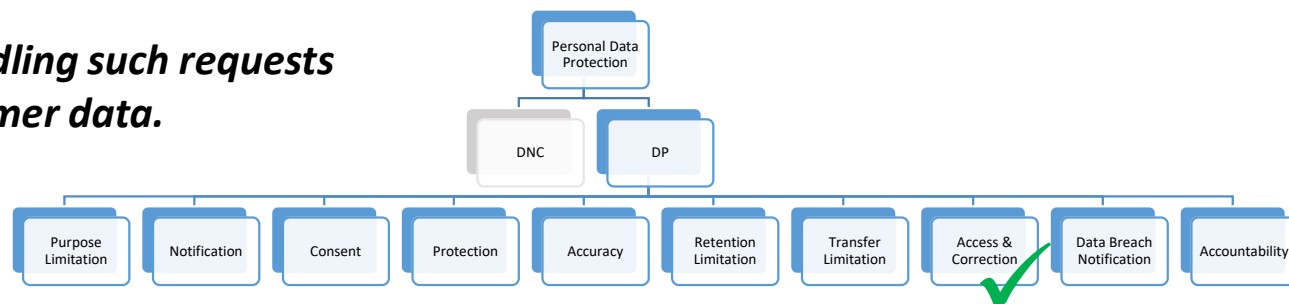
Data Access & Correction Obligations

Customer has the right to request / correct their personal data from RWS

Customers may do so by either:

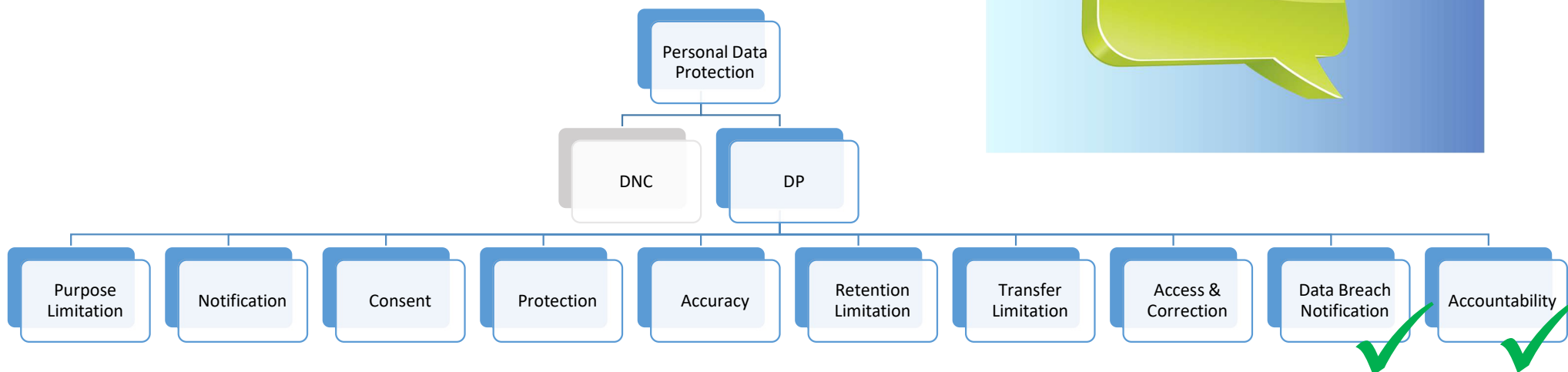
- Visiting the RWS Members Lounge in person
- Accessing the 'Personal Data Protection Statement' page on the RWS public website, completing the form, and submitting it to DPO via email.

BU shall follow their SOP when handling such requests to ensure proper handling for customer data.



Data Breach Notification Obligations

RWS is mandatory by law to notify data breach incidents to the PDPC and affected individuals



Handling Data Breaches – Event & Incident

Data breaches may lead to regulatory consequences

Data Incident Reporting Procedure MUST be triggered for managing any data related events/incidents at RWS

- ❖ All events and incidents must be handled in accordance with department's own internal incident reporting procedure
- ❖ All data-related events and incidents shall be recorded in the department's incident log

Data related Events :

Any event that concerns data and points to the **possibility** of data breach

- Employee discover document left unattended in office
- Employee concern about not updated data
- Employee feedback on data classification not practiced
- Information system security alerts about data stored beyond retention period

Data related Incidents :

Knowledge or reasonable belief that there has been unauthorized collection, use and disclosure of personal data

- Cyber attacks resulting in data stolen
- Unauthorized personal data access
- Disclosure of personal data to wrong personnel
- Sending of marketing materials to individuals who have withdrawn consent
- Accidental deletion of personal data which is to be retained



Handling Data Breaches SOP Timelines

Start

LTC shall alert HOD (Incident Response Lead) **immediately** upon discovery of data related event

Date Related Event

1. HOD record event details in department's incident log

Date Related Incident

HOD shall :

1. Perform preliminary assessment of the incident
2. **Notify IT, DPO, Legal, Compliance or Communication no later than 24 hours upon being alerted**
3. Work with the internal team to implement containment actions, assess consequences and root causes and take further necessary remediation actions

Accountability Obligations

RWS demonstrates accountability by:

1. Develop and implement departmental SOPs for data protection;
2. Communicating data protection policies to staff and fostering a culture of data protection through regular training and awareness programs;
3. Implement processes and practices that are necessary to meet your obligations under the PDPA.
4. Conduct Data Protection Impact Assessment (DPIAs) diligently

LTCs must contact DPO to initiate a DPIA before:

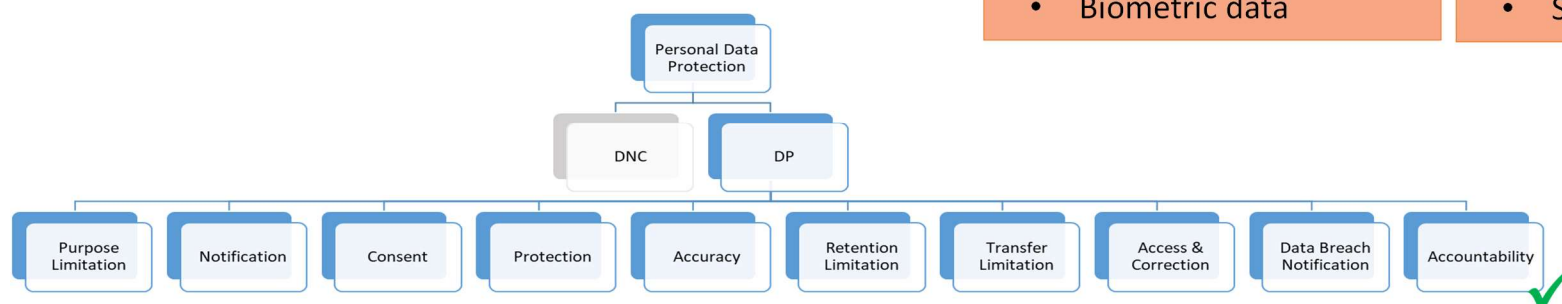
1. Changes to existing processes / systems handling personal data

2. Using sensitive personal data

- NRIC, FIN, Passport Data
- Health or medical data
- Children's data
- Financial data
- Criminal offence data
- Biometric data

3. Performing high risk processing

- Using new technologies, machine learning
- Large-scale Processing >500
- Online tracking
- Software applications
- Social networks



Summary

Do Not Call (DNC)

- Ensure **clear and unambiguous consent** is obtained before performing telemarketing calls & sending text messages

Purpose & Notification

- Ensure **customer is notified** of the purposes to collect, use or disclose their personal data. **Purpose must be reasonable**.

Consent

- Ensure consent obtained is **valid**, properly managed and stored during collection

Protection & Accuracy

- Ensure personal data are **handled with care and protected** at all time

Retention Limitation

- Ensure data are **securely disposed** when it is not longer needed



Consent Management

- Always consult DPO on how consent should be managed when BU need to collect personal data

Cross Border Data Transfer

- Always consult DPO before conducting activities involving cross border personal data transfer

Data Breach Notification

- Alert HOD (Incident Response Lead) immediately upon discovery of data related event / incident

Data Protection Impact Assessment

- Must contact DPO before handling any Sensitive Data / High Risk Processing



The End

Thank you for your participation

Signature: _____

Name: _____
(Name as in Passport/NRIC)

Passport/FIN/NRIC Number: _____
(Last 4 characters)

Designation: _____

Company Name: _____

Date: _____

