

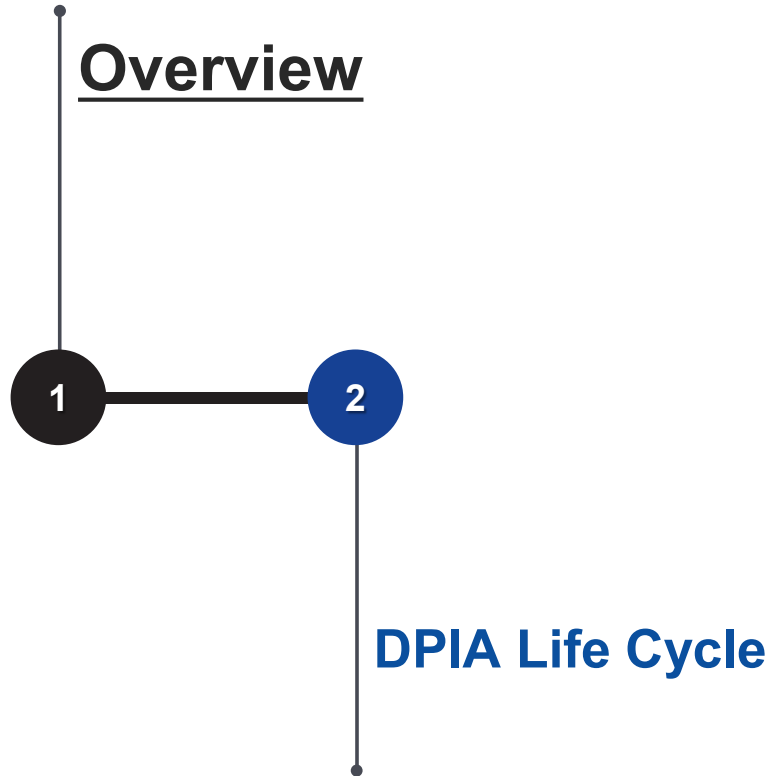
Data Privacy and Protection

Topic 6

Data Protection Impact Assessment

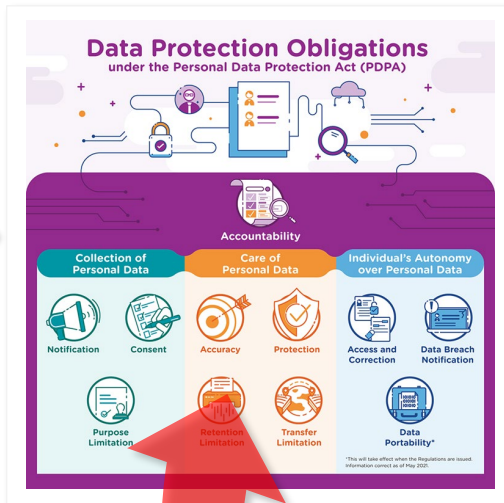


Contents



Data Protection Impact Assessment

11 main obligations of the PDPA



Develop and implement policies and practices to adhere to the PDPA

Data Protection Management Programme

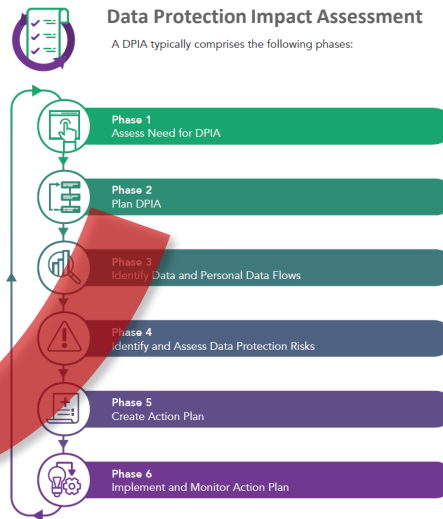
... builds a strong foundation for data protection within the organisation

- 1** Governance and Risk Assessment
- 2** Policy and Practices
- 3** Processes
- 4** Maintenance

Inputs to deciding on policies and practices to be implemented

Data Protection Impact Assessment

A DPIA typically comprises the following phases:



DPIA

- structured approach to identify data privacy risks
- implementing policies and practices to manage data privacy risks

Data Protection Impact Assessment



DPIAs can be conducted on systems and on processes.

The **key tasks** in a DPIA include

1. Identifying the personal data handled by the system or process
2. Identifying how the personal data flows
3. Identifying data protection risks
4. Addressing the identified risks
5. Checking to ensure that identified risks are adequately addressed

Data Protection Impact Assessment



Data protection risks are best addressed when the system or process is new or undergoing major changes.

Some examples of **when to conduct** a DPIA include the following, where personal data is being handled

1. Creating a new system
2. Creating a new process
3. Changing existing systems or processes
4. Changes to the organisational structure
5. Collecting new types of personal data

Data Protection Impact Assessment



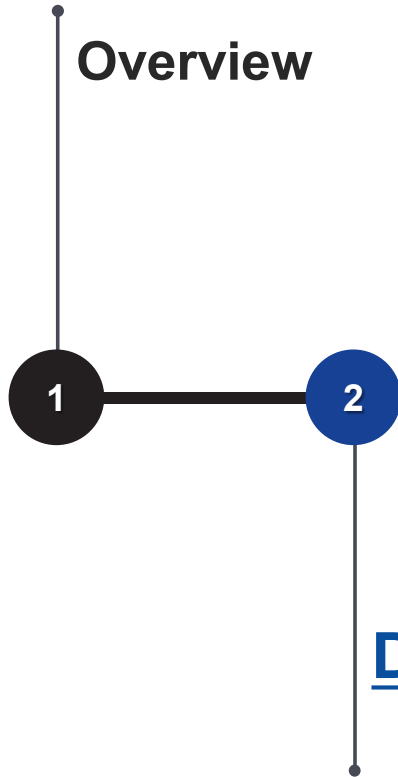
To address data protection risks effectively, a DPIA should involve relevant stakeholders and where needed, relevant external parties.

Data Protection Impact Assessment



Who	Role	Responsibilities
Project Manager (DPIA Lead)	Person in charge of the DPIA project	<p>Overall in-charge of the DPIA and could be supported by a DPIA team. Seeks input from relevant parties on:</p> <ul style="list-style-type: none"> • Data protection risks and challenges • Possible solutions to address the risks • Documents DPIA report • Monitors DPIA outcomes and reviews the DPIA
Data Protection Officer (DPO)	Enforcing the Data Protection policies	<p>Advises DPIA lead throughout the DPIA process, including providing support based on best practices</p> <ul style="list-style-type: none"> • Defining the risk assessment framework • Ensuring that DPIAs are conducted according to the organisation's policies • Assists in reviewing the DPIA report
Project Steering Committee	Management of organisation	<p>Commissions the DPIA Approves the DPIA report</p>
Others	Other organisational functions or external parties	<p>Provides input on potential risks and challenges, for example</p> <ul style="list-style-type: none"> • IT and Legal • Customer Service, Communications or Operations • Human Resource or Staff Capability

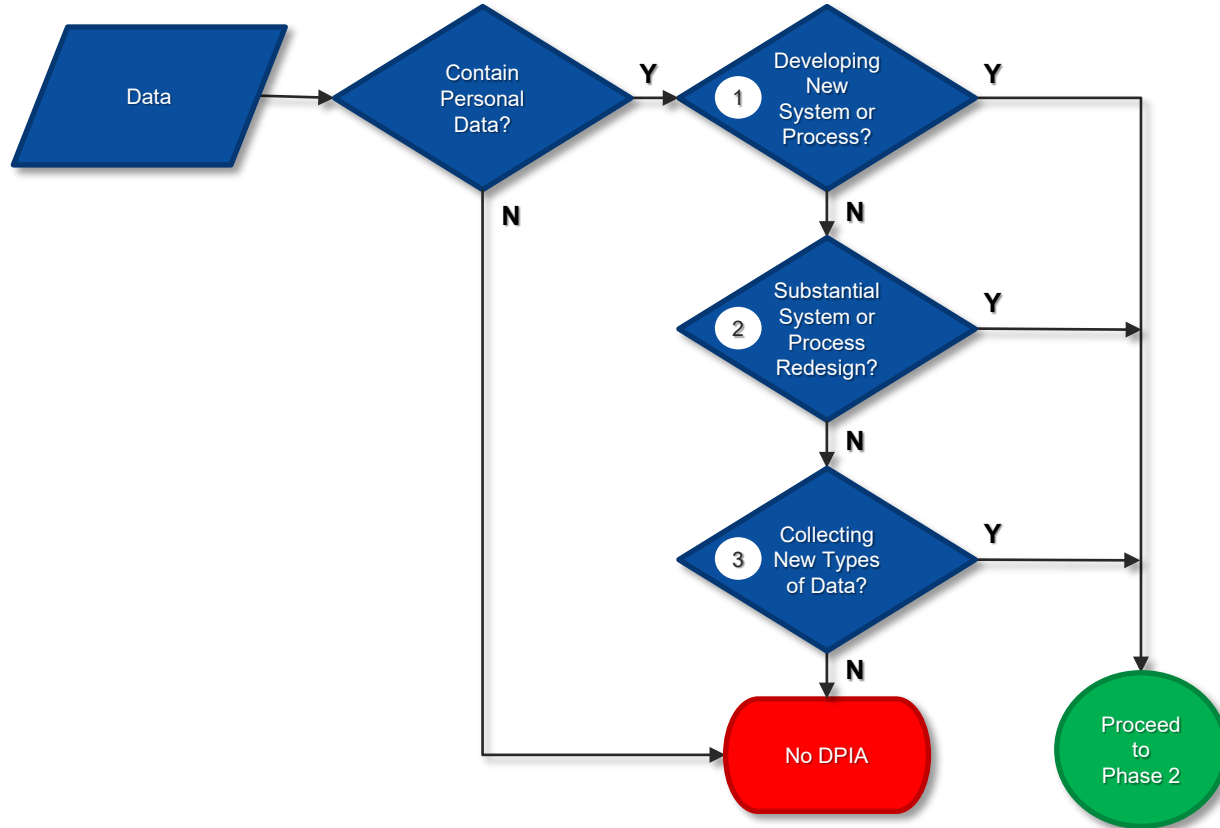
Contents



Data Protection Impact Assessment Life Cycle



Phase 1: Assess Need for DPIA



Phase 1: Assess Need for DPIA – Example



Organisation ABC is planning a marathon

- Website for individuals to register for the marathon
- Personal data collected through the website, stored in database
- ABC's management directs the website administrator to assess if a DPIA is needed
- Website administrator is assigned as DPIA lead
- There is a need to conduct a DPIA as it is a new system that handles personal data
- With management's approval, the DPIA lead proceeds to plan the DPIA

Phase 2: Plan DPIA



Project Description

- Overview of the project and reason for DPIA
- Key considerations



Scope of DPIA

- Detail of the specific system or process in scope



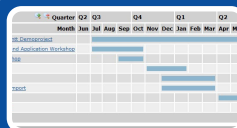
Define Risk Assessment Framework

- Risk assessment criteria
- Risk calculation method



Parties Involved

- Identify relevant internal or external stakeholders
- Approach in gathering stakeholder inputs

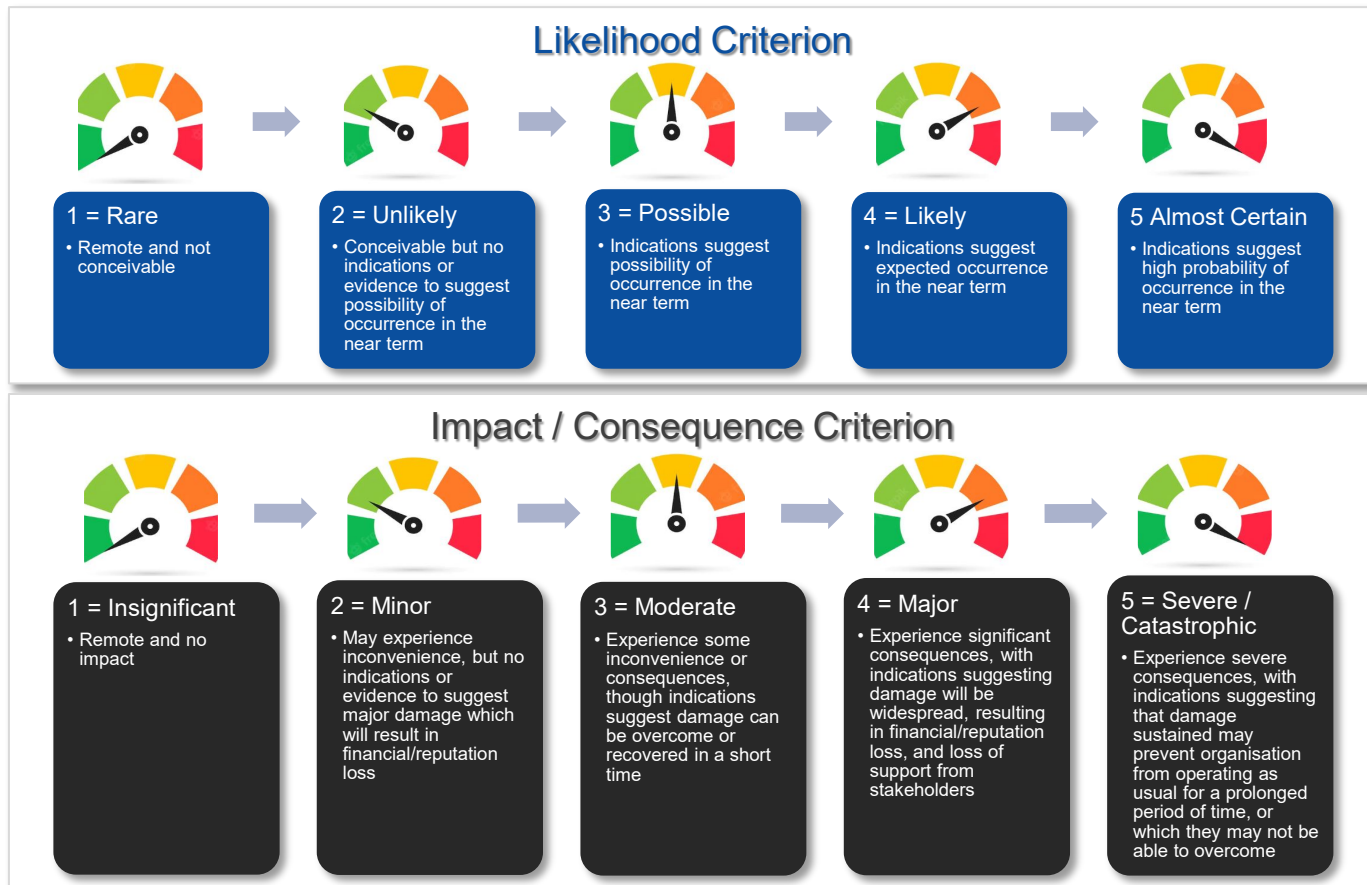


DPIA Timeline

- Overall DPIA timeline
- Key task timeline

Phase 2: Plan DPIA – Risk Assessment Framework

Personal data protection **risks** can be evaluated based on its **likelihood** and **impact**



Phase 2: Plan DPIA – Risk Assessment Framework

Quantitative Risk Ratings
 $\text{Risk} = \text{Likelihood} \times \text{Impact}$

Risk Matrix

		Consequence				
		Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Likelihood	5 Almost certain	Moderate 5	High 10	Extreme 15	Extreme 20	Extreme 25
	4 Likely	Moderate 4	High 8	High 12	Extreme 16	Extreme 20
	3 Possible	Low 3	Moderate 6	High 9	High 12	Extreme 15
	2 Unlikely	Low 2	Moderate 4	Moderate 6	High 8	High 10
	1 Rare	Low 1	Low 2	Low 3	Moderate 4	Moderate 5

Highest Risk Rating

Lowest Risk Rating

Risk Threshold
(immediate priority)

Phase 3: Identify Personal Data and Data Flows

DPIA lead would need to collate and review documentation related to the project (e.g., project plan, system functional specs) in order to determine how personal data is being collected, used or disclosed. DPIA lead should also consult stakeholders and conduct on-site inspections.



Identify various types of personal data handled and determine the purposes



Map the way that personal data flows through various stages

Phase 3: Identify Personal Data – Example



DPIA lead / Website administrator

- Consults the relevant project stakeholders (e.g., Planning team, IT, Finance, Marcom)
- Reviews any project relevant documentation

DPIA lead sets out to identify personal data touchpoints in the system

- Who has access to the various types of personal data?
- Where and how is the personal data being stored?
- How is the personal data being used?
- How long is the retention period and what are the disposal methods?

Phase 3: Identify Personal Data – Example (*Collection*)

A. Collection				
Interested participations register for the marathon and provide their particulars on the website. They are notified of the purposes of collection for the various types of personal data and are able to review the purposes in greater detail in ABC's data protection policy found on its website.				
Types of Personal Data	Purpose of Collection			
<ul style="list-style-type: none"> Full name/partial identification number Contact number Email address 	<ul style="list-style-type: none"> Identification and verification of participants before, during and after the event (e.g., goodie bag collection, printing and issuance of race bibs, lost and found). Communication purposes (e.g., contacting participants prior to race day to provide event details) 			
<ul style="list-style-type: none"> Age Gender 	<ul style="list-style-type: none"> Tracking of participants' profiles for future event planning purposes 			
<ul style="list-style-type: none"> Medical condition/history (if any) 	<ul style="list-style-type: none"> Provision of emergency medical support and services when required 			
<ul style="list-style-type: none"> Name of Next-of-Kin Contact number of Next-of-Kin 	<ul style="list-style-type: none"> Emergency contact purposes 			
Will individuals be notified of the purposes for which their information is collected, used and disclosed?	How is consent obtained?	Data Owner	Collection Source	Collection Medium
Yes, individuals will be notified of purposes at the point of collection on the website. These purposes can also be found in the data protection policy.	At point of information collection on the registration form, individual will click "I agree" before submitting form.	ABC organisation	Individual (interested marathon participant)	Electronic form on the website

Phase 3: Identify Personal Data – Example (*Storage & Use*)

B. Storage	
ABC stores the personal data collected on an electronic database. Access to the entire database is available only to certain individuals within the organisation.	
Physical Storage	Electronic Storage
NA	Once the registration form is submitted, personal data in the form would be transmitted and stored in ABC's electronic database. Access to the database and the level of access is limited to selected staff.

C. Use	
ABC uses the personal data collected for the purposes listed below. As different groups within ABC use the personal data for different purposes, their level of access to the personal data is dependent on their purposes.	
Users of Personal Data & Purpose of Usage	Access to Personal Data
<ul style="list-style-type: none"> • Contacting participants to provide information on marathon details (e.g., wet weather plans, route, reporting time), via emails and SMS <ul style="list-style-type: none"> ◦ These data processing activities are done in-house by the event planning team • Payment processing purposes <ul style="list-style-type: none"> ◦ Done in-house by the finance team • Printing of race bibs <ul style="list-style-type: none"> ◦ Prepared in-house, before sending to third party organisations for printing • Verifying identity of registered individuals for the collection of goodie bags/race bibs/T-shirts, prior to the event <ul style="list-style-type: none"> ◦ Details are processed and prepared in-house, before sending to third party organisation to arrange for distribution/collection • Verification and announcement of marathon winners/finishers <ul style="list-style-type: none"> ◦ Done in-house by the event planning team • Data profiling and trend analysis based on participants' age and gender <ul style="list-style-type: none"> ◦ Prepared in-house, with ABC anonymising the dataset 	<p>The following groups will be granted differing levels of access to personal data in the database:</p> <ul style="list-style-type: none"> • Event planning team <ul style="list-style-type: none"> ◦ Full access to personal data collected for communicating with participants, and for extracting relevant personal data to appointed third parties for processing. This includes participants' name, contact number and medical condition/history (only for provision of emergency medical support and services). • Finance team <ul style="list-style-type: none"> ◦ Access to full name and credit card details for payment processing purposes.

Phase 3: Identify Personal Data – Example (Disclosure, Retention & Disposal)

D. Disclosure	
ABC discloses certain personal data collected for the purposes listed below.	
External Parties and Purpose of Transfer/ Disclosure	Transfer Mode
<ul style="list-style-type: none">Appointed third party organisation will receive the full name and contact number of registered participants for the following purposes:<ul style="list-style-type: none">Printing and distributing goodie bags/race bibs/T-shirtsVerifying individuals during goodie bag collection (third party organisations may request for email confirmation as an added verification step)Paramedics, clinics or hospitals will receive (if requested) the full name, partial identification number and medical condition/history of registered participants for the purpose of:<ul style="list-style-type: none">Providing medical treatment (if needed)	Information will be emailed to the appointed third-party organisation.

E. Retention & Disposal	
ABC will cease to retain personal data according to its retention policy. The method of disposal is also specified in the retention policy.	
Retention Period	Disposal Methods
<ul style="list-style-type: none">ABC: 3 years from completion of eventAppointed third party organisations: 6 months from completion of event	<ul style="list-style-type: none">Digital files purged from database system, triggered by IT settingPhysical documents shredded in-house and disposed

Phase 4: Identify and Assess Risks

Having defined a risk framework and documented how personal data is being handled, the DPIA lead can now proceed to identify and assess personal data protection risks.



Complete a DPIA Questionnaire to assess the project against PDPA requirements



Identify areas in the personal data flow which could lead to a breach of the PDPA



Analyse the potential impact and likelihood of identified gaps and risks

Phase 4: Identify and Assess Risks – Example




In completing the DPIA Questionnaire, the DPIA lead's considerations could include

- What are the applicable PDPA requirements to be complied with?
- Is there an excessive collection of personal data?
- Are there sufficient measures in place to safeguard the personal data handled?
- Are staff aware of their roles and responsibilities?
- Are third party organisations aware of their personal data protection obligations?


Phase 4: Identify and Assess Risks – Example

Question	Response and Description of evidence/source	Personal data risks to individuals?	Risk Rating		
			Impact	Likelihood	Rating
Consent, Notification, Purpose Limitation					
Is consent obtained from individuals for any collection, use or disclosure of their personal data?	Yes. At point of collection, individuals are notified of the purposes of collecting, using or disclosing their personal data, and will have to select 'I agree' to them in order to submit their electronic registration form. However, the purpose of tracking participants' profiles for future planning is not explicitly disclosed.	As the dataset for tracking participants profiles will be anonymised for analysis, there is no risk to individuals.	1	1	1
Will the appointed 3 rd party organisations use the personal data disclosed to them in line with the intended purposes?	Partially. Organisation ABC will be appointing a 3 rd party organisation to print and distribute goodie bags/race bibs. As the 3 rd party organisation has not been appointed, the requirements to ensure that the personal data can only be used in line with ABC's intended purposes, have not been communicated.	Under the PDPA, personal data can only be used for the purposes to which individuals have consented. Hence, Organisation ABC will have to ensure that the contractual agreement with the appointed 3 rd party organisation will stipulate the purposes for which it may use the personal data.	4	3	12
Can individuals opt out from providing their personal data, and if so, is this easily understood by individuals?	Yes. The fields for age, gender, medical condition/history are optional. All other compulsory fields are marked by an asterisk, and individuals are not able to submit their registration form if they do not fill in a field with an asterisk. The compulsory fields are assessed to be the types of personal data minimally required in order for ABC to transact with the individual.	Individuals are able to provide the minimum personal data required to participate in the marathon.	2	2	4
Can individuals withdraw their consent for the collection, use and disclosure of their personal data?	There is currently no process established for this.	ABC is not in compliance with PDPA requirements which requires organisations to have a consent withdrawal process. This results in individuals having less control over their personal data and a potential delay for the organisation when responding to withdrawal requests.	5	3	15


Collection of Personal Data



Notification



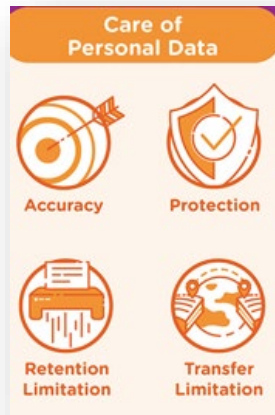
Consent



Purpose Limitation

Phase 4: Identify and Assess Risks – Example

Question	Response and Description of evidence/source	Personal data risks to individuals?	Risk Rating		
			Impact	Likelihood	Rating
Accuracy					
Is there a process in place to ensure that personal data collected is accurate and complete?	Yes. The form has logic checks for certain types of information. For example, the contact number field only allows 8-digit numbers, and the email address field requires the '@' symbol. The individual can also preview all information provided (and make changes) before submitting the form.	Low risk to individuals as there <u>are</u> steps taken to ensure that personal data collected is accurate and complete.	4	1	4
Protection					
Are there reasonable security arrangements to protect personal data? For example: <ul style="list-style-type: none">Is a security scan or penetration test scheduled to be conducted on the website before it is available to the public?Are users' direct access to the database strictly controlled? Are database activities logged?Are emails or documents containing personal data encrypted or password-protected? Are these methods reviewed periodically?	Yes. ABC's IT policy details the various measures it has in place to protect personal data in its possession or under its care. ABC also conducts periodic ICT security awareness training for its staff. However, the IT policy does not prescribe the frequency at which security measures should be reviewed. There should be a process in place for regular monitoring or review of IT security measures to ensure they are up to date, as it is currently maintained on an ad-hoc basis by the IT team.	Personal data of individuals may be exposed if the website or database in which it is stored contains vulnerabilities. There needs to be a regular review to ensure that the website collecting personal data and the electronic database storing the personal data has reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.	4	3	5
Are third party organisations that personal data is disclosed to clear about the security arrangements they need to put in place to protect the data?	Partially. As the 3 rd party organisation has not been appointed, ABC's requirements or expectations to protect personal data have not been communicated.	Under the PDPA, organisations and their data intermediaries are responsible for protecting the personal data under the organisation's possession or control. As the 3 rd party organisation may not be aware of or have the proper safeguards in place to protect ABC's personal data, individuals are more likely to be at risk of personal data breaches.	4	4	16



Phase 4: Identify and Assess Risks – Example



Question	Response and Description of evidence/source	Personal data risks to individuals?	Limitation	Notification	
			Risk Rating		
			Impact	Likelihood	Rating
Retention					
Is there a data retention policy for the personal data stored in the database? (Describe the data retention procedures, purposes, retention periods, etc.)	Yes. ABC has in place a data retention policy which will be maintained by the event planning department. ABC will cease to retain the personal data of individuals 3 years from the completion of the marathon by shredding and disposing physical documents and purging digital files. This will be triggered by an IT setting. Under ABC's retention policy, third party organisations would have to cease to retain personal data 6 months from completion of event.	ABC will have to ensure that the contractual agreement with the appointed 3 rd party organisation covers the stipulated retention (and data disposal) policy for personal data. Otherwise, the appointed 3 rd party organisation may be holding on to personal data that is no longer required by ABC and individuals would be at risk of harm or impact should the 3 rd party organisation suffer a data breach.	2	2	4
Data Breach Notification					
Has Organisation ABC established the criteria for a notifiable data breach?	Yes. Organisation ABC's DPO has included in its data protection policy a section on the data breach notification based on the Personal Data Protection (Data Breach Notification) Regulations 2021. Staff have been made aware of what to do in the event of a data breach, and to ensure that it is brought to attention so that the DPO may identify whether the data breach calls for notifying affected individuals or PDPC.	Organisation ABC will have to ensure that staff are aware of the criteria of a notifiable data breach, and that the DPO is informed in the event of a data breach so as to determine whether it is notifiable.	4	2	8

Phase 4: Identify and Assess Risks – Example



Question	Response and Description of evidence/source	Personal data risks to individuals?	Risk Rating		
			Impact	Likelihood	Rating
Accountability					
<p>Are staff aware of ABC's data protection policies and practices?</p> <p>Do the data protection policies cover the obligations of the PDPA?</p>	<p>Yes. New staff that process personal data undergo training and are required to read ABC's handbook on data protection policies and undertake a short test. This extends to the event planning and finance teams. Staff that join the event planning team also have to read up on the department's specific data protection policies and practices in relation to the database storing personal data (e.g., methods to anonymise personal data for statistical analysis purposes).</p> <p>The event planning department also discusses personal data protection issues (e.g., responding to withdrawal of consent, access and correction requests) during meetings.</p> <p>At the organisation level, regular communication mailers on data protection-related matters (e.g., new data protection practices) are sent to all staff.</p>	<p>All staff are aware of Organisation ABC's data protection initiatives.</p> <p>However, in view that some functions are outsourced, ABC should ensure that the appointed 3rd party organisation handling their personal data is also well aware of its data protection responsibilities. This could be stipulated in the contractual agreement.</p>	2	2	4

Phase 5: Create Action Plan

Based on the various personal data protection risks identified, the DPIA lead can now create an Action Plan, which outlines the specific tasks to be taken in order to address those risks.



List the critical tasks to be taken in order to address the various data protection risks identified



Assign the action owners responsible to address the identified risks



Formulate a timeline for when specific tasks need to be completed and determine its priority

Phase 5: Create Action Plan – Example



In developing the action plan, the DPIA lead's considerations include

- What are the risk treatment options, taking into consideration the risk assessment?
- What constraints does the organisation face?
- What other legal requirements does the organisation need to consider?
- What are the pros and cons for each recommendation or proposed solution?
- How can the proposed solutions be integrated within the organisation's business?

Phase 5: Create Action Plan – Example

	Description of Risk/Gap	Remarks	
1	No consent withdrawal process.	ABC needs to develop and implement a consent withdrawal process as PDPA requires organisations to have a consent withdrawal process.	
	Action Plan	Implementation Timeline	Action Owner(s)
a.	Develop and implement a consent withdrawal request process for carrying out these requests (including developing a consent withdrawal form) and determine interim measures.	1 month	Project Manager, DPO
b.	Train relevant staff within ABC with the new process.	2 weeks from completion of item (a)	Project Manager, DPO
c.	Ensure that appointed 3 rd party organisation is aware, so that they can refer participants to ABC if needed.	Upon appointment of 3 rd party organisation	Project Manager

Phase 5: Create Action Plan – Example

	Description of Risk/Gap	Remarks	
2	No process to review and ensure that reasonable security arrangements are in place to safeguard personal data to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.	ABC needs to ensure that security measures to protect personal data collected via the website and stored in the database, are kept relevant and enforced.	
	Action Plan	Implementation Timeline	Action Owner(s)
a.	Establish a process to conduct regular reviews on security arrangements to ensure relevance and establish how each review should be carried out. This should include holding regular compliance and audit checks.	3 months	IT department, Project Manager
b.	Third party organisations would need to be apprised of and put in place the required security measures. These requirements should be included in all 3 rd party contracts, and reviewed regularly (e.g., when contracts are being renewed).	Upon appointment of 3 rd party organisation	Project Manager, Legal

Phase 5: Create Action Plan – Example

	Description of Risk/Gap	Remarks	
3	<p>Third party organisation unaware of ABC's requirements or expectations to protect personal data that are disclosed to them by ABC.</p> <p>ABC has yet to communicate its requirements or expectations to protect personal data to the 3rd party organisation.</p>	<p>Under the PDPA, organisations and their data intermediaries are responsible for protecting personal data under the organisation's possession or control. Given that the 3rd party organisation may not be aware of or have proper safeguards in place to protect personal data, individuals are more likely to be at risk of personal data breaches.</p>	
	Action Plan	Implementation Timeline	Action Owner(s)
a.	<p>Draft contractual agreements with appointed 3rd party organisation stating the required security measures to safeguard personal data, ensuring that:</p> <ul style="list-style-type: none"> • The vendor will provide adequate level of care, protection and security of personal data in accordance with the PDPA and ABC's requirements • The vendor has in place and will activate the data breach management plan should a data breach occur • The vendor will cease to retain personal data according to the stated retention policy in the agreement and destroy the personal data upon the expiry of the agreement or as stated in the agreement. 	Upon appointment of 3 rd party organisation	Project Manager, Legal, IT department

Phase 6: Implement Action Plan and Monitor Outcome



DPIA Report

- Document the whole DPIA process
- Reviewed by DPO
- Approved by Project Steering Committee



Action Plan Implementation

- Implement the plan by respective Action Owners
- Monitor outcome by Project Manager



Maintain DPIA

- Subsequent developments to the project
- Technology or security developments
- External environmental changes

Contents

