GUIDE TO

DATA PROTECTION IMPACT ASSESSMENTS

SG:DIGITAL

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

CONTENTS

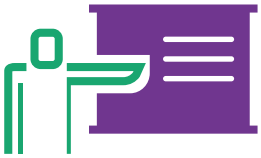
INTRODUCTION 4

PART I: DATA PROTECTION IMPACT ASSESSMENTS 6
When to conduct a DPIA? 7
Who should be involved in a DPIA? 8

PART II: DPIA LIFE CYCLE 10
Phase 1 — Assess Need for DPIA 12
Phase 2 — Plan DPIA 13
Phase 3 — Identify Personal Data and Personal Data Flows 14
Phase 4 — Identify and Assess Data Protection Risks 18
Phase 5 — Create an Action Plan 26
Phase 6 — Implement Action Plan and Monitor Outcomes 29

ANNEX 30
Annex A: Risk Assessment Framework 31
Annex B: Sample DPIA Questionnaire 33

INTRODUCTION



INTRODUCTION

The Data Protection Provisions of the Personal Data Protection Act ("**PDPA**") comprises 11 main obligations which organisations must comply with when undertaking activities relating to the collection, use or disclosure of personal data[1]. In the course of meeting these obligations, organisations are required to develop and implement policies and practices that are necessary for the organisation to comply with the PDPA[2]. These policies and practices[3] should eventually be evident through organisations' Data Protection Management Programme ("**DPMP**")[4].

In deciding on the policies and practices to be implemented in compliance with the PDPA, organisations are encouraged to conduct a Data Protection Impact Assessment ("**DPIA**")[5]. A DPIA involves identifying, assessing and addressing personal data protection risks based on the organisation's functions, needs and processes. In doing so, an organisation would be better positioned to assess if their handling of personal data complies with the PDPA or data protection best practices, and implement appropriate technical or organisational measures to safeguard against data protection risks to individuals.

This guide provides an outline of key principles and considerations for organisations, especially those without any measures or tools to address specific personal data protection risks, on conducting a DPIA for systems and processes. The practices suggested in this guide are for general information and are non-exhaustive. In particular, the examples herein are for illustrative purposes only. Adopting the suggestions in this guide does not mean that one will be in compliance with the PDPA. An organisation should determine the most appropriate steps for conducting its own DPIAs, and could consider whether the suggestions in this guide can be adapted for its specific circumstances (e.g. sectoral, business or operational requirements).

1 *While there are 11 obligations under the PDPA, the Data Portability Obligation is not yet in force.*
2 *Sections 11 and 12 of the PDPA.*
3 *Policies set the direction and course of action by the organisation to meet its obligations under the PDPA, while practices are specific processes in place to operationalise policies.*
4 *A DPMP is a systematic framework to help organisations establish a robust personal data protection infrastructure. It generally sets out an organisation's management policies, application of processes and practices, and roles and responsibilities of staff in the handling of personal data. Refer to PDPC's Guide to Developing a Data Protection Management Programme for more information.*
5 *A DPIA is also a key component of taking a Data Protection by Design ("**DPbD**") approach, in which organisations consider the protection of personal data from the earliest possible design stage, and throughout the operational life cycle, of the new system, process, product or service. This way, the appropriate safeguards to protect personal data would have been embedded within.*

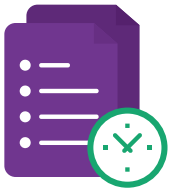
PART I: DATA PROTECTION IMPACT ASSESSMENTS

DATA PROTECTION IMPACT ASSESSMENTS

DPIAs can be conducted on systems (e.g. public-facing websites, cloud storage platforms, Customer Relationship Management ("**CRM**") systems) and processes (e.g. undergoing a health screening and receiving the medical report, purchasing an item from an online portal and receiving it from a courier).

The key tasks in a DPIA include:

1. Identifying the personal data handled by the system or process, as well as the reasons for collecting the personal data
2. Identifying how the personal data flows through the system or process
3. Identifying data protection risks by analysing the personal data handled and its data flows against PDPA requirements or data protection best practices
4. Addressing the identified risks by amending the system or process design, or introducing new organisation policies
5. Checking to ensure that identified risks are adequately addressed before the system or process is in effect or implemented



WHEN TO CONDUCT A DPIA?

Data protection risks are best addressed when the system or process is (i) new and in the process of being designed or (ii) in the process of undergoing major changes. Introducing changes to address data protection risks after the design of a process or system has been finalised or implemented will likely lead to increased cost and effort. Some examples of when to conduct a DPIA include:

1. Creating a new system that involves the handling of personal data (e.g. new website that collects personal data)
2. Creating a new process, including manual processes, that involves the handling of personal data (e.g. receptionist collecting personal data from visitors)
3. Changing the way that existing systems or processes handle personal data (e.g. redesign of the customer registration process)
4. Changes to the organisational structure that affects the department handling personal data (e.g. mergers and acquisition, restructuring)
5. Collecting new types of personal data (e.g. collecting new information about existing customers)

Individual DPIAs should be conducted for each system or process that involves the handling of personal data (including the linking or sharing of personal data with other parties). For the purpose of this guide, the term "projects" will be used to refer to such systems or processes.

It is also recommended that a DPIA be conducted for multiple projects that are similar in purpose, scope and context. For instance, a retail organisation that intends to digitise the collection of consumer data across all its branches may conduct one DPIA exercise that covers the handling of consumers' personal data across branches.

WHO SHOULD BE INVOLVED IN A DPIA?

An effective DPIA should involve relevant stakeholders from various functions of the organisation (e.g. the project manager, the organisation's Data Protection Officer, IT department) and where needed, relevant external parties (e.g. subject matter experts), to identify, assess and address the data protection risks. The person leading the DPIA (henceforth "**DPIA lead**") should ideally be the Project Manager or the organisation's Data Protection Officer ("**DPO**").

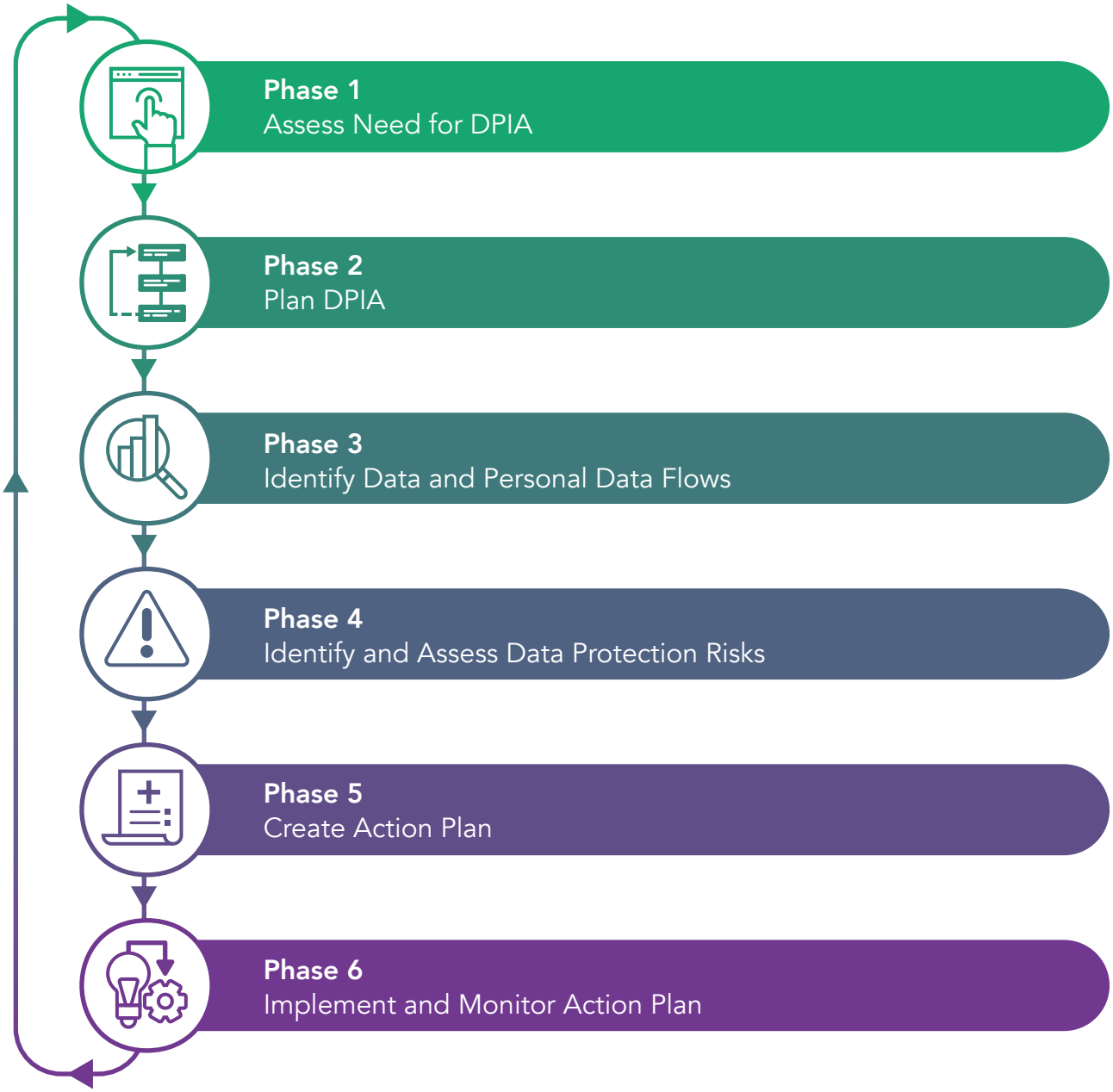
The table below lists out typical roles and responsibilities of key parties involved in the DPIA. This guide will assume that the DPIA lead is the Project Manager.

Who is involved?	Who are they?	Role in DPIA
Project Manager	Person in charge of the project	• DPIA lead, overall in-charge of the DPIA and could be supported by a DPIA team • Assesses the need for DPIA, plans the DPIA and conducts the DPIA • Identifies and seeks input from relevant stakeholders, including project team, on: o Potential data protection risks and challenges to the project from an implementation perspective o How identified personal data protection risks should be addressed and possible solutions o Documents DPIA report (which includes proposing detailed action plan) for management's approval o Monitors DPIA outcomes and reviews the DPIA when there is a change in risks to personal data protection
Data Protection Officer ("**DPO**")	Person responsible for creating and enforcing the Data Protection policies within the organisation May tap on DPO networks or associations for resources or advice from other DPOs to guide the DPIA lead in carrying out the DPIA	• Advises DPIA lead throughout the DPIA process, including: o Identifying and mitigating identified data protection risks by providing support based on best practices adapted to organisation's needs and circumstances o Defining and applying the risk assessment framework o Ensuring that DPIAs are conducted according to the organisation's policies and recommends improvement to DPIA methodology based on industry best practices o Reviewing DPIA report prior to submission to management • Develops the templates/DPIA questionnaire necessary to complete the DPIA • Assists in reviewing the DPIA when there is a change in risks to personal data protection
Project Steering Committee	Management of organisation that approved the project	• Commissions the DPIA • Approves the risk assessment framework • Approves the DPIA plan, and proposed action plans and solutions arising from the DPIA
Others	Other organisational functions or departments that have some level of involvement in the project, external parties such as subject matter experts or even potentially affected individuals, where needed.	• Provides input on potential risks and challenges to the project with respect to their function. For example: o IT and Legal: Advising the DPIA lead on possible IT solutions and security/legal risks in implementing measures to protect personal data. This may also include advising on potential challenges on system design and development. o Customer Service, Communications or Operations: Advising the DPIA lead on possible consumer impact (e.g. in terms of usability) if the DPIA outcomes warrant a change to consumer interaction or day-to-day operations. o Human Resource or Staff Capability: Advising on the appropriate training programmes or resources should the DPIA outcomes require staff to be able to carry out new data protection measures or activities.

PART II:
DPIA LIFE CYCLE

DPIA LIFE CYCLE

A DPIA typically comprises the following phases:



PHASE 1 — ASSESS NEED FOR DPIA

Before conducting the DPIA, organisations should assess whether there is a need for a DPIA with the following considerations. First, the DPIA lead and the DPO would have to assess whether there is a need for a DPIA by determining if the project involves personal data (i.e. the collection, use, transfer, disclosure or storage of personal data). If the project does not involve personal data, then a DPIA is not necessary.

If it has been determined that the project involves personal data, the threshold questions below can be used to further assess the need for a DPIA. If the answer is "yes" to any of these questions, then a DPIA should be conducted[6]. If the answer is "no" to both questions, the DPIA lead should assess again when there is a change in risks associated with handling of personal data in the project.

1. Is a new system or process being introduced, developed or implemented? For example, new IT systems or manual processes that involve the handling of personal data (e.g. receptionist collecting personal data from visitors, disposal of physical documents containing personal data, submitting of physical medical claims).

2. Is an existing system or process being reviewed or substantially redesigned? For example, a redesign of an operational process workflow that involves different groups of users handling personal data.

3. Is the organisation starting to collect new types of data? For example, a change of business model which may include collecting new types of personal data about existing customers.

Note: Organisations could establish a more detailed set of threshold questions to assess the need for conducting a DPIA to suit organisational processes, legislative and/or project requirements.

Once the decision is made to conduct a DPIA, the DPIA lead should proceed to plan the DPIA in consultation with the DPO. The DPO should also advise the DPIA lead throughout the conduct of the DPIA.

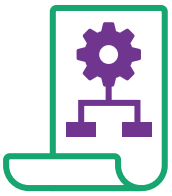
The scenario below illustrates how an organisation may decide to conduct a DPIA on a new system:

[6] *Or reviewed, if a DPIA had been conducted previously.*

Case Example 1

Organisation ABC is planning a marathon and intends to set up a website for individuals to register for the marathon. Personal data collected through the website will be stored on ABC's database. As personal data is involved, ABC's management directs the website administrator to assess if there is a need for a DPIA on this system that comprises the website and database.

The website administrator, as the DPIA lead, assesses that 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

In establishing the key activities or steps needed to conduct the DPIA, the DPIA lead should cover the following aspects:

Project description — An overview of the project (e.g. objective/background, organisation department/functions involved, timeline), why a DPIA is needed and key considerations surrounding the DPIA, if any.

Scope of DPIA — Describe in detail the specific system or process on which a DPIA needs to be carried out.

Define risk assessment framework or methodology — This includes establishing the risk assessment criteria and methods of calculating risk[7].

Parties involved — Identify relevant internal departments/functions or external stakeholders (e.g. subject matter experts, consultants, regulatory authorities or customers) whose inputs or views would have to be sought during consultation or interview sessions, and describe how their views would be sought.

DPIA timeline — Provide an estimate of the time required for key tasks and overall timeline for conducting the DPIA.

[7] *Refer to Annex A for an example of a risk assessment framework. Organisations should use a risk assessment framework appropriate for their objectives and needs. Risk assessments can vary depending on the organisation's circumstances, such as available resources and information, and may also be qualitative or quantitative.*

PHASE 3 — IDENTIFY PERSONAL DATA AND PERSONAL DATA FLOWS

To identify and map personal data involved in the project, the DPIA lead would need to collate and review documentation related to the project in order to determine how personal data is being collected, used or disclosed as part of the project. Examples of documentation include the project plan, contracts with third parties, assessment reports and functional specifications of the system. The DPIA lead should also consult with the project team and relevant departments or functions to ensure comprehensiveness and accuracy. On-site inspections of the project together with ground personnel should also be conducted where possible.

The DPIA lead can then proceed to:

1. Identify various types of personal data handled (or envisaged to be handled) in relation to the specific project and determine the organisation's purposes for collecting, using or disclosing them; and
2. Map the way that personal data flows through various stages or touchpoints of the project (e.g. considering operational workflows or business processes), across its life cycle (i.e. from collection to storage and/or disposal).

The following case example highlights some considerations the DPIA lead should have when identifying the various types of personal data involved and mapping the personal data flows:

Case Example 1A

As the DPIA lead, the website administrator consults the relevant project stakeholders (e.g. marathon event planning team, IT team, finance team, marketing and communications team) and reviews relevant documentation of past marathon events. In doing so, the DPIA lead would have a good understanding of the types of personal data that would be involved in the project and the purposes for which the data will be collected, used or disclosed.

Next, the DPIA lead sets out to identify data touchpoints in the system and maps out how personal data flows across its life cycle (e.g. by examining instances where personal

data is collected, stored, used, disclosed, retained and disposed). The DPIA lead also considers the following points to aid the mapping of personal data:

- Who has access to the various types of personal data (internal and external parties)?
- 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? Are similar expectations placed on external parties and if so, are they aware?

The table below illustrates how the DPIA lead has identified and mapped out personal data flows for the project.

<table>
<tr><th colspan="5">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 Organisation ABC's data protection policy found on its website.</th></tr>
<tr><th>Types of Personal Data</th><th colspan="4">Purpose of Collection</th></tr>
<tr><td>• Full name/partial identification number
• Contact number
• Email address</td><td colspan="4">• 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)</td></tr>
<tr><td>• Age
• Gender</td><td colspan="4">• Tracking of participants' profiles for future event planning purposes</td></tr>
<tr><td>• Medical condition/history (if any)</td><td colspan="4">• Provision of emergency medical support and services when required</td></tr>
<tr><td>• Name of Next-of-Kin
• Contact number of Next-of-Kin</td><td colspan="4">• Emergency contact purposes</td></tr>
<tr><th>Will individuals be notified of the purposes for which their information is collected, used and disclosed?</th><th>How is consent obtained?</th><th>Data Owner</th><th>Collection Source</th><th>Collection Medium</th></tr>
<tr><td>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.</td><td>At point of information collection on the registration form, individual will click 'I agree' before submitting form.</td><td>Organisation ABC</td><td>Individual (interested marathon participant)</td><td>Electronic form on the website</td></tr>
</table>

B. Storage

Organisation 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 Organisation ABC's electronic database. Access to the database and the level of access is limited to selected staff.

C. Use

Organisation 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

• Contacting participants to provide information on marathon details (e.g. wet weather plans, route, reporting time), via emails and SMS
  o These data processing activities are done in-house by the event planning team
• Payment processing purposes
  o Done in-house by the finance team
• Printing of race bibs
  o 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
  o 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
  o Done in-house by the event planning team
• Data profiling and trend analysis based on participants' age and gender
  o Prepared in-house, with Organisation ABC anonymising the dataset
	The following groups will be granted differing levels of access to personal data in the database:
	
	• Event planning team
	  o 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
	  o Access to full name and credit card details for payment processing purposes.

D. Disclosure
Organisation ABC discloses certain personal data collected for the purposes listed below.

External Parties and Purpose of Transfer/ Disclosure	Transfer Mode
• Appointed third party organisation will receive the full name and contact number of registered participants for the following purposes: o Printing and distributing goodie bags/race bibs/T-shirts o Verifying 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: o Providing medical treatment (if needed)	Information will be emailed to the appointed third party organisation.

E. Retention & Disposal
Organisation 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
• Organisation ABC: 3 years from completion of event • Appointed third party organisations: 6 months from completion of event	• Digital files purged from database system, triggered by IT setting • Physical documents shredded in-house and disposed

Note: Organisations should customise the above fields to align with organisational or project requirements.

As the DPIA lead maps out the flow of personal data throughout the project, he/she may start noticing areas or gaps for improvement (e.g. ensuring reasonable security measures to protect the electronic database, training staff to ensure only necessary personal data is extracted and sent to appointed third party organisations, and ensuring no unauthorised disclosure of personal data). Refer to the **Guide to Developing a Data Protection Management Programme** for more examples on how personal data flows could be mapped.

PHASE 4 — IDENTIFY AND ASSESS DATA PROTECTION RISKS

Having documented how personal data is being handled, the DPIA lead can proceed to identify and assess personal data protection risks by:

1. Completing a DPIA questionnaire to assess the project against PDPA requirements and/or data protection best practices[8];
2. Identifying areas in the personal data flow which could lead to a breach of the PDPA (e.g. loss of personal data) or are gaps when compared against industry best practices; and
3. Analysing the potential impact and likelihood of identified gaps and risks based on the pre-defined risk framework.

As projects vary across types (e.g. systems, digital or manual processes) and project stages (i.e. new projects, existing projects undergoing major changes), there is no one-size-fits-all method to identify, assess or address data protection risks. DPIA leads would need to consider the organisation's specific circumstances in assessing data protection risks, and may also have to retrace earlier steps or activities undertaken in earlier phases to obtain more information or clarify certain data handling processes at various stages of the project.

The following case example illustrates some considerations in identifying and assessing data protection risks:

Case Example 1B

In responding to the DPIA questionnaire to identify data protection risks, the DPIA lead's considerations could include:

- What are the applicable PDPA requirements to be complied with for activities relating to the collection, use or disclosure of personal data? Are there policies and practices to meet these requirements?
- Is there an excessive collection of personal data, i.e. beyond what is required for the stated purposes?

[8] *The DPIA questionnaire would be typically developed by the DPO. Nonetheless, the DPIA lead could review the questionnaire to ensure that it covers uses of persona data or data processing activities, that may be identified only during Phase 3.*

- What are the best practices that could be followed for activities relating to the collection, use or disclosure of personal data? Should they be reflected in the organisation's policies and practices?
- Are there sufficient measures in place to safeguard the personal data handled?
- Are staff aware of their roles and responsibilities? Have they undergone relevant training and are they kept updated of the organisation's data protection policies and practices?
- Are third party organisations aware of their personal data protection obligations?

The table below illustrates some possible questions and responses[9].

Question	Response and description of evidence/source	What are the personal data risks to individuals?	Risk Rating		
Consent, Notification, Purpose Limitation			Impact	Livelihood	Rating
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. The purposes are also documented in the data protection policy. However, note that 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
Are the purposes for which personal data is collected, used or disclosed, considered reasonable?	Yes, an internal assessment was conducted to ensure that the purposes are reasonable and are detailed in event planning documents.	NA	1	1	1

[9] *This particular risk assessment is based on a sample risk framework (See Annex A).*

Question	Response and description of evidence/source	What are the personal data risks to individuals?	Risk Rating		
Are the purposes for the collection, use or disclosure of personal data documented?	Yes, the purposes are detailed in event planning documents.	NA	1	1	1
Will the appointed third party organisations use the personal data disclosed to them in line with the intended purposes?	Partially. Organisation ABC will be appointing a third party organisation to print and distribute goodie bags/race bibs. As the third 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 third 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 Organisation 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.	Organisation 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

Question	Response and description of evidence/source	What are the personal data risks to individuals?	Risk 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 are 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: • 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 to track unauthorised activities or anomalies? • Are emails or documents containing personal data encrypted or password-protected? Are these methods reviewed periodically to ensure that they are recognised by the industry and are relevant and secure?	Yes. Organisation 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	15

Question	Response and description of evidence/source	What are the personal data risks to individuals?	Risk Rating		
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 third party organisation has not been appointed, Organisation 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 third party organisation may not be aware of or have the proper safeguards in place to protect Organisation ABC's personal data, individuals are more likely to be at risk of personal data breaches.	4	4	16
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. Organisation 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.	Organisation ABC will have to ensure that the contractual agreement with the appointed third party organisation covers the stipulated retention (and data disposal) policy for personal data. Otherwise, the appointed third 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 third party organisation suffer a data breach.	2	2	4

Question	Response and description of evidence/source	What are the personal data risks to individuals?	Risk Rating		
Is there a data disposal policy? (Describe the processes involved to ensure that data is securely disposed of.)	Yes. Under Organisation ABC's disposal policy, upon cessation of retention, storage media is securely deleted, erased or destroyed before redeploying, exchanging or disposing of the storage. Physical destruction of storage media such as degaussing and incinerating may also be employed where secure deletion, erasure or deletion of personal data stored on the media is not possible (e.g. with faulty storage media).	Organisation ABC will have to ensure that such policies are communicated internally and enforced. ABC must also ensure that any third party organisations engaged are contractually obliged to follow the same policies. Otherwise, such data may be stored beyond their retention period and expose ABC and its customers to risk of 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

Question	Response and description of evidence/source	What are the personal data risks to individuals?	Risk Rating		
Are there processes in place to ensure that customers are promptly notified in the event of a notifiable data breach?	Yes, Organisation ABC's data protection policy has included means of contacting customers via their preferred form of communications. ABC's policy has also included the content of what should be in the notification, including facts of the data breach, data breach management and its remediation plan.	Organisation ABC will have to ensure that the communications are correctly done, and that no further breach of data occurs.	2	2	4
Are there processes in place to ensure that PDPC is promptly notified in the event of a notifiable data breach?	Yes, Organisation ABC's data protection policy has included triggers for notifying PDPC in the event that the criteria for a notifiable data breach are met.	Organisation ABC will have to ensure that the criteria are adhered to and that data breaches are promptly flagged internally.	2	2	4
Are there processes in place to ensure prompt remediation in the event of a data breach?	Yes, Organisation ABC has included in its data protection policy a risk management process to identify and rectify the source of the data breach.	Organisation ABC will have to actively review this process to ensure that risks are eliminated.	4	2	8

Question	Response and description of evidence/source	What are the personal data risks to individuals?	Risk Rating		
Accountability					
Are staff aware of Organisation ABC's data protection policies and practices? Do the data protection policies cover the obligations of the PDPA?	Yes. New staff that process personal data undergo training, and are required to read Organisation 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). The event planning department also discusses personal data protection issues (e.g. responding to withdrawal of consent, access and correction requests) during meetings. At the organisation level, regular communication mailers on data protection-related matters (e.g. new data protection practices) are sent to all staff.	All staff are aware of Organisation ABC's data protection initiatives. However, in view that some functions are outsourced, ABC should ensure that the appointed third party organisation handling their personal data is also well aware of its data protection responsibilities. This could be stipulated in the contractual agreement.	2	2	4

Note: The above is not an exhaustive list of DPIA questions for the project. Refer to Annex B for more sample DPIA questions.

PHASE 5 — CREATE AN ACTION PLAN

In this phase, the DPIA lead would need to propose how the identified data protection risks should be addressed. Documented in the form of an action plan, the DPIA lead should also indicate the action owner(s) responsible for the implementation of specific recommendations (such as technical or organisational measures), monitoring of implementation outcomes, as well as implementation timelines. As good practice, the action plan should also provide a contact point for responding to queries regarding the DPIA process or arising from implementing the action plan.

An organisation's approach to developing the action plan should be informed by the risk assessment (in Phase 4), as well its specific circumstances (e.g. operational or resource constraints and other legal or regulatory requirements). This would impact how the identified data protection risks would be addressed (e.g. removing the source of risk, spreading the risk with another party via risk financing and contracts, taking the risk by informed decision), and the implementation timeline of proposed solutions in the action plan. For instance, data protection risks may be prioritised based on their likelihood and impact levels, instead of implementing all the recommendations at once. Nonetheless, all recommendations and justifications should be documented for future reference.

The following case example illustrates how the DPIA lead could document proposed solutions to address identified data protection risks.

Case Example 1C

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

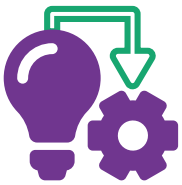
- What are the risk treatment options, taking into consideration the defined risk assessment framework? What is the organisation's risk appetite?
- What operational or resource constraints does the organisation face?
- What other legal or regulatory requirements does the organisation need to consider?
- What are the pros and cons for each recommendation or proposed solution? Are there other alternatives to be considered and why are they not recommended?
- How can the proposed solutions be integrated within the organisation's project management practices or processes?

Having considered the above, the DPIA lead then draws up an action plan. An extract of the action plan is illustrated:

	Description of gap/risk	Remarks	
1	No consent withdrawal process.	Organisation 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 Organisation ABC with the new process.	2 weeks from completion of item B	Project Manager, DPO
c.	Ensure that appointed third party organisation is aware, so that they can refer participants to ABC if needed.	Upon appointment of third party organisation	Project Manager

	Description of gap/risk	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.	Organisation 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 third party contracts, and reviewed regularly (e.g. when contracts are being renewed).	Upon appointment of third party organisation	Project Manager, Legal

	Description of gap/risk	Remarks	
3	Third party organisation unaware of Organisation ABC's requirements or expectations to protect personal data that are disclosed to them by ABC. ABC has yet to communicate its requirements or expectations to protect personal data to the third party organisation.	Under the PDPA, organisations and their data intermediaries are responsible for protecting personal data under the organisation's possession or control. Given that the third 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.	
	Action Plan	**Implementation timeline**	**Action Owner(s)**
a.	Draft contractual agreements with appointed third party organisation stating the required security measures to safeguard personal data, ensuring that: • The vendor will provide adequate level of care, protection and security of personal data in accordance with the PDPA and Organisation ABC's requirements; • The vendor has in place and will activate the data breach management plan should a data breach occur; and • 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 third party organisation	Project Manager, Legal, IT department



PHASE 6 — IMPLEMENT ACTION PLAN AND MONITOR OUTCOMES

The DPIA lead is now ready to document the whole DPIA process (i.e. how the DPIA was scoped, planned and carried out, findings and proposed action plan) into a DPIA report[10]. This report should be reviewed by the organisation's DPO to ensure that the proposed action plan is in line with the organisation's policies and contains effective data protection practices. Once the report has been reviewed by the DPO, the DPIA lead should submit the report to the Project Steering Committee, and seek approval to implement the action plan.

Once approved, the respective action owners can start to implement the action plan. The project owner should also monitor the outcomes of the action plan to ensure that identified personal data protection risks are addressed as planned and risks to personal data continue to be managed responsibly.

When there is a change in risks associated with handling of personal data in the project, the existing DPIA (in particular the action plan outcomes) would need to be reviewed and updated where needed so that any new gaps or risks to individuals' personal data can be addressed[11]. Examples of when risks can change include:

1. Subsequent developments to the project (e.g. changes to the purposes or context for the project, the type of personal data collected, how the processing is conducted)
2. Technology or security developments (e.g. when a system may face new security vulnerabilities)
3. Broader environmental changes (e.g. legislative amendments)

[10] *The report should also provide background or contextual information about the project and explain the approach for treating data protection risks.*

[11] *This would entail following the steps of the DPIA process from Phase 1. In retracing the steps, DPIA leads may consult new groups of internal or external stakeholders that have become relevant to the project, factoring in new data touchpoints in mapping personal data flow and assessing newly identified and/or existing data protection risks, among others.*

ANNEX

ANNEX A: RISK ASSESSMENT FRAMEWORK

The significance of data protection risks could be evaluated based on its likelihood and impact. Defining the risk criteria should include establishing the specific criteria for each level of likelihood and impact, their respective scales and the criteria for risk acceptance[12]. Organisations should use risk assessment frameworks that are appropriate for their objectives and needs. When defining risk criteria, organisations could consider legal and regulatory requirements, industry best practices or guidelines and project-specific requirements.

Below is an example of a risk framework where the data protection risk is assessed by multiplying its projected or estimated level of likelihood and impact to derive a quantitative risk rating. Each criterion is based on a five-point scale. This means that "1" is the lowest possible risk rating and "25" is the highest possible risk rating. The risk acceptance criterion is set at "15" and data protection risks with risk ratings of "15" and above would be given immediate priority.

Likelihood criterion				
1 = Rare	**2 = Unlikely**	**3 = Possible**	**4 = Likely**	**5 = Almost Certain**
Remote and not conceivable	Conceivable but no indications or evidence to suggest possibility of occurrence in the near term	Indications suggest possibility of occurrence in the near term	Indications suggest expected occurrence in the near term	Indications suggest high probability of occurrence in the near term

Impact criterion				
1 = Insignificant	**2 = Minor**	**3 = Moderate**	**4 = Major**	**5 = Severe**
Remote and no impact	May experience inconvenience, but no indications or evidence to suggest major damage which will result in financial/ reputation loss	Experience some inconvenience or consequences, though indications suggest damage can be overcome or recovered in a short time	Experience significant consequences, with indications suggesting damage will be widespread, resulting in financial/reputation loss, and loss of support from stakeholders	Experience severe consequences, with indications suggesting that damage sustained may prevent organisation from operating as usual for a prolonged period of time, or which they may not be able to overcome

[12] *Depending on the risk ratings, organisations can then evaluate the data protection risks and prioritise their action plans accordingly.*

Examples of data protection risks

In identifying personal data protection risks, organisations may wish to refer to this list for some broad examples:

- Inefficient or ineffective processes to handle personal data
- Insufficient or absence of security controls
- When data accuracy is compromised
- Inadequate notification to individuals regarding the collection, use and disclosure of their personal data
- When consent is not obtained for purposes for which personal data is used
- Insufficient review and monitoring of data protection processes
- Inadequate safeguards on third party organisations processing personal data
- Personal data collected is more than what is required for intended purposes
- When organisation does not have a retention policy and personal data is retained longer than necessary for intended legal or business purposes
- When organisation does not have a policy and process for the safe disposal of personal data

Examples of risk treatment options

Depending on the risk rating, organisations may adopt certain approaches in proposing or developing solutions and action plans that aim to control the risks. For instance, organisations may decide to eliminate a certain risk by not starting or continuing with the activity that gave rise to the risk in the first place, or changing the likelihood of a risk by putting in place measures that would greatly reduce its occurrence. More examples of such approaches are:

- Taking the risk by informed decision
- Increasing the risk in order to pursue an opportunity
- Removing the source of risk
- Spreading out the risk with another party or parties (including contracts and risk financing)

ANNEX B: SAMPLE DPIA QUESTIONNAIRE

The questionnaire below illustrates how the DPIA lead can assess the project against a range of PDPA requirements and data protection best practices, and identify gaps or risks related to personal data protection. DPOs can develop or modify the questions based on organisational processes and/or specific project requirements, as well as data protection best practices.

Questions	
Content	
1	Is consent obtained from individuals for any collection, use or disclosure of their personal data?
2	Is personal data being collected directly from individuals? If not, what measures are in place to ensure that the individual had consented or is deemed to have consented to the collection, use or disclosure of their personal data?
3	Is there a process to obtain fresh consent from individuals to use their personal data for a new or different purpose, if applicable?
4	Are individuals able to opt out from providing their personal data, and if so, is this easily understood by individuals?
5	Is there a process for individuals to withdraw their consent for the collection, use or disclosure of their personal data?
6	Are individuals informed of the consequences of withdrawing their consent?
Notification	
7	Are individuals notified of the purposes of collecting, using or disclosing of their personal data?
Purpose	
8	Is the amount and type of personal data collected, used and disclosed, limited to the purposes made known to the individual?
9	Are the purposes for the collection, use or disclosure of personal data documented?
Accuracy	
10	Is there a process in place to ensure that personal data collected is accurate and complete?
Access and Correction	
11	Is there a process to receive, review and respond to access or correction requests?
Protection	
12	Are there reasonable security measures and safeguards in place to protect personal data in relation to the system or process, throughout the personal data life cycle? This includes administrative, physical or technical measures.
13	Does the system or process produce hardcopy documents that contain personal data? If yes, describe the security measures in place to process and safeguard these documents.
14	Is personal data disclosed to third party organisations in Singapore?

	Questions
15	Is personal data disclosed to third party organisations further disclosed to other third party organisations?
16	Are there contractual agreements to ensure these third party organisations have reasonable security measures in place to safeguard personal data?
17	Are third party organisations assessed for their data protection practices before they are selected?
18	Is there a process to receive and respond to data breach or related data protection incidents?
Retention	
19	Is there an established data retention policy? (Describe the data retention procedures, purposes, retention periods, etc.)
20	Is there a process for the destruction or archival of personal data?
Transfer	
21	Is personal data transferred to third party organisations outside Singapore? If so, how does the organisation ensure that these third party organisations have a comparable standard of data protection as the PDPA and PDP Regulations?
Data Breach Protection	
22	Is there an established data breach notification policy, with clear criteria set out for a notifiable data breach?
23	Is there a clear communication plan to affected individuals?
24	Is there a clear communication plan to PDPC?
25	Is there a clear remediation plan, including identifying the cause of the data breach and how to rectify it?
Accountability	
26	Have staff been trained regarding the protection of personal data by informing them of organisational and project-specific data protection policies, procedures and best practices?
27	Are roles and responsibilities relating to data protection in this project clearly defined?

Note: The above list of criteria and questions should be modified to suit organisational processes, legislative and/or project requirements.

#SGDIGITAL

Singapore Digital (SG:D) gives Singapore's digitalisation efforts a face, identifying our digital programmes and initiatives with one set of visuals, and speaking to our local and international audiences in the same language.

The SG:D logo is made up of rounded fonts that evolve from the expressive dot that is red. SG stands for Singapore and :D refers to our digital economy. The :D smiley face icon also signifies the optimism of Singaporeans moving into a digital economy. As we progress into the digital economy, it's all about the people — empathy and assurance will be at the heart of all that we do.

BROUGHT TO YOU BY

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE