pdpc

PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE


# GUIDE ON ACTIVE ENFORCEMENT

*Revised on 1 October 2022*

Supported by

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

In support of

SG:DIGITAL

# CONTENTS

# INTRODUCTION

# OVERVIEW OF FRAMEWORK

The Personal Data Protection Act 2012 ("**PDPA**") establishes the baseline standard for data protection for private sector organisations. The PDPA confers enforcement powers to the Personal Data Protection Commission ("**PDPC**") to investigate and utilise enforcement powers in relation to breaches of the PDPA, including data breach incidents.

A data breach incident ("**incident**") refers to an incident exposing personal data in an organisation's possession or under its control to the risks of *unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks*. It also includes the loss of any storage medium or device on which personal data is stored in circumstances where unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.

One of the PDPC's objectives is to maintain the trust between consumers and organisations by ensuring appropriate enforcement actions are taken against organisations that are found to be in breach of the PDPA. In doing so, the PDPC strives to ensure a balance between the protection of personal data and the enabling of data collection and processing by organisations in new ways employing new technologies.

On 1 February 2021, amendments to the PDPA included the increase of the maximum financial penalty for breaches of the PDPA. Accordingly, when considering the appropriate enforcement outcome, the PDPC is guided by four key objectives:

1. To respond effectively to breaches of the PDPA where the focus is on those that adversely affect large groups of individuals and where the data involved are likely to cause significant harm to the affected individuals;

2. To be proportionate and consistent in the application of enforcement actions on organisations that are found in breach of the PDPA;

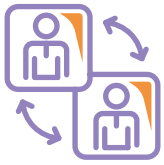
3. Where penalties imposed serve as an effective deterrent to those that risk non-compliance with the PDPA; and

4. To ensure that organisations that are found in breach take proper steps to correct gaps in the protection and handling of personal data in its possession and/or under their control.

The scope of the PDPA is wide. Consequently, not all complaints and incidents can be fully investigated. This guide on the PDPC's Active Enforcement Framework ("**Framework**") targets both consumers as well as organisations that handle personal data. It reiterates the PDPC's general approach to maximise the use of facilitation and mediation in seeking a resolution between the complainant and the organisation concerned, and articulates the approach in the exercise of the PDPC's enforcement powers so as to act effectively and efficiently. This guide outlines how the PDPC handles data protection complaints, investigates incidents and the types of enforcement outcomes that the PDPC may impose in various circumstances[1]. Finally, this guide explains the general principles for determining the financial penalty amount imposed for cases where the organisations are found to be in breach of the PDPA.

[1]*It should be noted that while the Framework outlines the types of enforcement outcomes, it is by no means exhaustive. The PDPC reserves the right to exercise its discretion to impose other enforcement outcomes as it deems fit.*

This guide provides insights into the PDPC's enforcement policy. However, it should not be construed to limit or restrict the PDPC's administration and enforcement of the PDPA. The provisions of the PDPA and any regulations or rules issued thereunder will prevail over the Framework in the event of any inconsistency. This guide should be read in conjunction with other advisory guidelines issued by the PDPA from time to time, which explain in detail the obligations that organisations have to comply with under the PDPA.



# FACILITATION AND MEDIATION

The PDPC recognises that personal data protection issues may arise in the context of disputes of a private nature between an individual and an organisation. These may be better resolved by both parties through facilitation, mediation or other modes of alternative dispute resolution.

Therefore, the PDPC would, as a first step, facilitate communication between the parties so that they may resolve the issue(s) raised. If the issue(s) remains unresolved, and the PDPC is of the opinion that any complaint by an individual against an organisation may be more appropriately resolved by mediation, the PDPC may, without the consent of the complainant and the organisation, refer the matter for mediation under a dispute resolution scheme, pursuant to section 48G(1) of the PDPA.

If the PDPC is of the view that facilitation and/or mediation may not be appropriate, the PDPC may initiate full investigations early. Such cases may involve disclosure of personal data on a large scale and/or involve data which are likely to cause significant harm to the affected individuals.

More information about how the PDPA is generally enforced and its approach to resolving complaints via facilitation and mediation can be found in the Advisory Guidelines on Enforcement of the Data Protection Provisions.

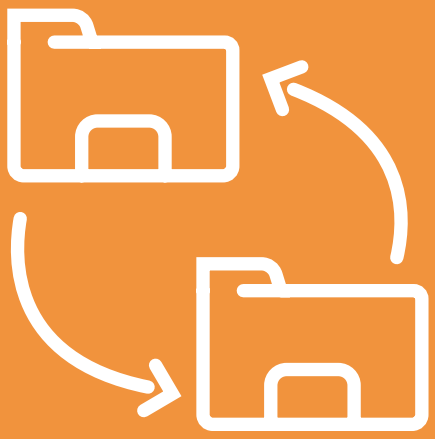
# GOALS OF THE PDPC IMPOSING ENFORCEMENT OUTCOMES

The PDPC is committed to increasing data protection standards across the board for all organisations. In imposing enforcement outcomes, the PDPC aims to encourage organisations to be in compliance with the PDPA. To assist organisations, the PDPC issues advisory guidelines concerning the PDPA and selected topics on data protection.

Decisions on investigations ("**Decisions**") into PDPA breaches by organisations and voluntary undertakings provided by organisations to the PDPC are published on the PDPC's website. Confidential information may be redacted at the PDPC's discretion. By disclosing the Decisions publicly, the PDPC, as a personal data protection regulator, seeks to:

1. Increase public awareness of the obligations under the PDPA;
2. Publicise guidance and good practices on how to comply with the PDPA to build and foster consumer trust and confidence in organisations' handling of personal data in a digital world;
3. Encourage organisations to embed an accountability culture towards data protection;
4. Deter conduct and/or practices which may contravene organisational obligations pursuant to the PDPA; and
5. Instil public confidence in the PDPC as an effective personal data protection regulator.

The Framework aims to continue to enable the most efficient resolution of personal data protection disputes and incidents that are brought to the PDPC's attention. The Framework builds upon the principle of accountability that underlies the PDPA and promotes the positive behaviours that the PDPC would like to see in organisations with respect to their handling of personal data and related incidents. The various enforcement outcomes are further elaborated in **Part III: Types of Enforcement Outcomes**.



# INVESTIGATION PROCESS

# INVESTIGATION PROCESS

Details about the investigation process and powers of the PDPC can be found in the Advisory Guidelines on Enforcement of the Data Protection Provisions.

A summary of the investigation process is shown below:

Incident surfaced to the PDPC via complaint, self-notification etc.

↓

Determine if the incident involves the collection, use or disclosure of personal data*. For example, the PDPC generally considers the following types of data, on its own, to be personal data for enforcement purposes:

1. Full name
2. NRIC number or FIN (Foreign Identification Number)
3. Passport number
4. Personal mobile telephone number

**Personal data is defined in section 2 of the PDPA as data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access.*

**No** ↓

No investigation will be initiated as case facts do not involve a breach of data protection obligations.

**Yes** ↓

1. Refer to Facilitation/Mediation;
2. Refer to other regulatory authorities (MAS, MOH, etc.); or
3. Refer to the PDPC's Investigations Team.

**When case is taken up for investigations** ↓

**Investigations — Fact-gathering process**

1. Notice to produce documents and information
2. Interviews/Statements
3. Site visits

←

**PDPC Decision**

# TYPES OF ENFORCEMENT OUTCOMES

# TYPES OF ENFORCEMENT OUTCOMES

The enforcement outcomes that follow an investigation are as follows:

1. **Suspension or discontinuation** of the investigation;
2. **Voluntary undertaking;**
3. **Breach findings,** which may result in the following outcomes:

   (i) **No breach;**
   (ii) **Warning;**
   (iii) **Directions;**
   (iv) **Financial penalties; or**
   (v) **Directions and financial penalties.**

***Suspension or Discontinuation of the Investigation***

Suspension or discontinuation of investigations into potential breaches of the PDPA may take place in various situations. In general, the PDPC may consider discontinuing investigations in situations where the impact is assessed to be **low or limited**. The PDPA provides that the PDPC may suspend, discontinue or refuse to conduct an investigation under section 50 if it thinks fit, including but not limited to any of the following circumstances:

1. The complainant has not complied with a direction under section 48G(2);

2. The parties involved in the matter have mutually agreed to settle the matter;

3. Any party involved in the matter has commenced legal proceedings against the other party in respect of any contravention or alleged contravention of the PDPA by the other party;

4. The PDPC is of the opinion that the matter may be more appropriately investigated by another regulatory authority and has referred the matter to that authority;

5. The PDPC is of the opinion that:
   (i) A complaint is frivolous, or vexatious, or is not made in good faith; or
   (ii) Any other circumstances warrant refusing to conduct, suspending or discontinuing the investigation (e.g. where there is permanent cessation of business or where other Singapore laws take precedence over the PDPA).

In such cases, the PDPC may also issue an advisory notice to the organisation(s) involved.

The advisory notice is not a finding of a breach of the PDPA but serves to highlight areas where an organisation can improve in, so as to increase their level of compliance with the PDPA. For instance, as part of the advisory notice, the PDPC may provide the organisation with some guidance on best practices when sending out mass external emails.

**Example: Where a mass email was sent with email addresses visible to every recipient**

Retail store ABC sent email invitations to 50 members to promote the launch of its new products and invite members to a members-only preview sale. However, retail store ABC failed to insert their email addresses in the Bcc: field, and instead, inserted the email addresses and in some instances, accompanying names, in the To: field. This allowed the email addresses and/or accompanying names to be disclosed to all recipients of that email. A member of the retail store, Ms C, lodged a complaint with the PDPC, alleging that retail store ABC had used and disclosed her personal data without her consent.

Retail store ABC admitted that a procedural lapse caused the breach and it was aware that the email addresses and/or accompanying names should have been inserted in the Bcc: field. It had sent an apology email to the affected members. As the impact of the breach to individuals was assessed to be low and the email addresses and/or accompanying names were disclosed to a small group of individuals (i.e. contained only within members of retail store ABC), the PDPC is likely to discontinue the investigation and issue an advisory notice to retail store ABC.

**Example: Where mobile numbers were disclosed via Messaging Group Chat**

Company EFG is a job agency which matches individuals to potential job opportunities. Mr D has registered his particulars with the company for employment purposes. Company EFG recently employed a temporary staff to assist with matching job opportunities with individuals. To speed up the matching process, the temporary staff created a Messaging Group Chat ("**Group**") to inform 10 job-seekers registered with company EFG of a new position. Mr D was added to the Group. He subsequently lodged a complaint with the PDPC, alleging that company EFG had used and disclosed his personal data (i.e. mobile number) without his consent.

During the course of investigations, company EFG informed the PDPC that it had failed to ensure that its staff was properly trained to comply with the obligations under the PDPA, and the staff should not have created the Group without the consent of its registered job-seekers. When it discovered the incident, company EFG had promptly deleted the Group and sent an apology email to the affected registered job-seekers. As the impact of the breach was assessed to be low and the mobile numbers were disclosed to a small group of individuals (i.e. contained only within registered job-seekers), the PDPC is likely to discontinue the investigation and issue an advisory notice to company EFG.

**Example: Where personal data is inadvertently disclosed to only one other party without consent**

Organisation HIJ, an F&B service provider, has a membership programme where individuals who would like to enjoy discounts could sign up for yearly renewable memberships. One month before Ms E's membership expired, organisation HIJ decided to send her an email about membership renewal.

However, as the process was done manually, organisation HIJ inserted the details of another member in the email meant for Ms E. The details comprised the name, mobile number, membership number and expiration date of the membership of the other member. Ms E received the email containing the wrong details and lodged a complaint with the PDPC, alleging that organisation HIJ had disclosed a third party's personal data to her.

Organisation HIJ admitted that it was a human error and that it would enhance its system to prevent future occurrences. Organisation HIJ also reached out to Ms E and the other member to resolve matters amicably. As the impact of the breach was assessed to be low and the details of the other member were only disclosed to one party, (i.e. Ms E), the PDPC is likely to discontinue the investigation and issue an advisory notice to organisation HIJ.

**Example: Where there are ongoing legal proceedings involving the organisation(s) which relate to the incident**

Ms A entered the premises of organisation CDE without permission. Organisation CDE's policy stipulates that details of trespassers/unauthorised individuals into its premises may be posted on its notice boards for security purposes. Consequently, organisation CDE grabbed a screenshot of Ms A via its CCTV footage and posted it on its notice boards within its premises.

When Ms A came to know of this, she lodged a complaint with the PDPC, alleging that organisation CDE had used and disclosed her personal data without consent. Concurrently, Ms A pursued a civil suit against organisation CDE for defamation. The defamation suit stemmed from similar facts.

In this case, there were ongoing legal proceedings involving Ms A and organisation CDE relating to the incident. Hence, the PDPC would likely discontinue the investigation.

**Example: Where the complaint was frivolous or vexatious**

Ms B frequents salon XYZ for beauty services. On one occasion, a dispute over the signed package between Ms B and the salon ensued in an acrimonious exchange over an instant messaging ("**IM**") application. Ms B then posted screenshots of the IM exchanges containing details of the package on salon XYZ's social media page. The details included Ms B's name, contact number, date of birth, address and occupation.

In a bid to protect its reputation, salon XYZ replied to Ms B's posting but did not disclose further personal data of Ms B not found within the package details. Ms B lodged a complaint with the PDPC, alleging that salon XYZ had used and disclosed her personal data on the social media platform without consent.

During the course of investigations, it was made clear that Ms B was the party who first disclosed her personal data on the social media platform. Salon XYZ did not disclose further personal data of Ms B when responding to her posts on the social media platform. In this case, as salon XYZ had not disclosed Ms B's personal data, Ms B's complaint would be regarded as frivolous or vexatious, and the PDPC would likely discontinue the investigation.

### *Voluntary Undertaking (section 48L of the PDPA)*[2]

Under certain circumstances, the PDPC may accept a written voluntary undertaking from the organisation. The organisation's request in writing to the PDPC to invoke the voluntary undertaking process must be made soon after the incident is known, i.e. either upon commencement of investigations and/or in the early stages of investigations. The voluntary undertaking will take effect from when the executed voluntary undertaking is returned to the PDPC by the organisation. The organisation's execution of a voluntary undertaking does not amount to an admission of breach of the PDPA.

The voluntary undertaking is intended to allow organisations to be given the opportunity to implement their remediation plan in relation to the incident within a specified time. The possibility of a voluntary undertaking may arise when:

1. The organisation is able to demonstrate that it has accountable policies and practices in place (for example, an organisation which is IMDA Data Protection Trustmark certified, has effective monitoring and breach management systems etc.); and

2. The organisation is ready with a remediation plan and is committed to implement it forthwith. The remediation plan should explain:
   (i) The likely cause(s) of the incident;
   (ii) The proposed steps to address the cause(s); and
   (iii) The targeted completion date(s) of the proposed steps.

[2]*Please refer to Part V: Voluntary Undertaking in the Advisory Guidelines on Enforcement of the Data Protection Provisions.*

The PDPC may consider accepting such a request from the organisation if it assesses that a voluntary undertaking achieves a similar or better enforcement outcome more effectively and efficiently than a full investigation. A key consideration is the effectiveness of the remediation plan and the organisation's readiness to implement it forthwith. The acceptance of a voluntary undertaking is solely within the PDPC's discretion.

The request by the organisation **must** be accompanied with a remediation plan and should state how the requirements leading to the possibility of a voluntary undertaking will and/or have been met. The organisation will not be given additional time to produce the remediation plan. The PDPC may work together with the organisation to pinpoint areas of improvement for the remediation plan, specifically in relation to the incident. In this manner, the organisation's data protection knowledge can be heightened as well.

The voluntary undertaking will typically:

1. Describe the incident that the organisation is involved in;

2. Include a remediation plan that sets out the measures that the organisation will take to voluntarily rectify the cause(s) of the incident within a specified time. Such measures may include steps to reduce recurrence of the incident as well as putting in place monitoring and reporting processes, audits and policy/process reviews; and

3. Contain the organisation's acknowledgement to provide related reports of the organisation's and/or third party to the PDPC if and when requested.

The voluntary undertaking will be published by the PDPC[3]. The PDPC may consider redacting matters that are confidential upon the organisation's request. To be clear, publication by the PDPC is distinct from any commitment by the organisation to publish the undertaking or publicise its terms on other platform(s).

The PDPC is **unlikely** to accept a voluntary undertaking request in any of, but not limited to, the scenarios below:

1. The organisation refutes responsibility for the incident;
2. It is a repeat incident entailing similar cause(s) of breach;
3. The remediation plan does not explain how compliance with the PDPA may be achieved in relation to the incident;
4. The organisation requests for extended time to produce a remediation plan; and
5. The breach is wilful or egregious.

Where an organisation withdraws its request for the voluntary undertaking, the PDPC may proceed with a full investigation of the incident and/or impose any other enforcement outcome as it deems fit.

Where an organisation is found not to have complied with any term(s) of the voluntary undertaking, the PDPC may take action that it thinks fit in the circumstances to ensure the compliance of the organisation with the term(s) of the voluntary undertaking. This includes (i) issuing directions to enforce the terms of the voluntary undertaking; or (ii) instituting or resuming a full investigation into the incident which could lead to the imposition of directions and/or a financial penalty. The PDPC may still publicise the voluntary undertaking while a full investigation of the incident is being conducted.

[3]*Please refer to Section 22 (Publication of voluntary undertakings) of the Personal Data Protection (Enforcement) Regulations 2021.*

**Example: Where the organisation requests the PDPC to accept a voluntary undertaking, is Trustmark-certified and is in possession of a remediation plan**

Company GHI's server had been subjected to unauthorised access by an alleged perpetrator. As a result, data belonging to its customers comprising names and email addresses were likely to have been accessed by the perpetrator. When contacted by the PDPC for the purpose of investigations, company GHI admitted that the incident might have occurred due to the use of a shared administrative account for its database. Company GHI subsequently requested to provide a voluntary undertaking to the PDPC and submitted a comprehensive remediation plan together with the request.

Company GHI's remediation plan comprised, amongst others, plans to introduce a two-factor authentication, halt the practice of shared login credentials to the administrative account, make its administrative account more secure, and improve its alert system to detect possible intrusions. Company GHI had also obtained the IMDA Data Protection Trustmark certification.

In this case, company GHI had been cooperative. There was also a remediation plan put in place by company GHI to ensure that the direct cause(s) of breach were addressed and other measures introduced to enhance the security of its IT system. Therefore, the PDPC is likely to accept the request by company GHI to provide a voluntary undertaking to the PDPC.

***Full Investigation Process: Breach Findings with Warning, Directions and Financial Penalties***

Typically, the PDPC encourages organisations to resolve the issues with the complainant(s) directly. The PDPC has an established facilitation and mediation process to encourage Data Protection Officers ("**DPOs**") and complainants to resolve the matter amicably[4]. However, for incidents assessed as **high impact**, the PDPC will launch a full investigation process immediately. These are usually incidents where a large number of individuals was affected and/or the personal data disclosed could cause significant harm. Such investigation process is likely to be prolonged depending on the level of cooperativeness from the organisation(s) involved.

Once a breach by the organisation is determined by the PDPC, the following enforcement outcomes may be imposed on the organisation:

(i) **Warning;**
(ii) **Directions;**
(iii) **Financial penalties; or**
(iv) **Directions and financial penalties.**

Upon completion of the full investigation and dependant on the enforcement outcome, the PDPC will issue a Preliminary Decision which sets out the proposed direction(s) to be issued and/or proposed financial penalty notice to be imposed. The organisation may choose to make representations with relevant supporting documents enclosed. Before issuing the Final Decision, the PDPC will consider the representations presented for the findings made in the Preliminary Decision.

The Final Decision will be published by the PDPC. More details on the investigation process are available in the Advisory Guidelines on Enforcement of the Data Protection Provisions.

Financial penalties will be elaborated in **Part IV: Financial Penalties**.

[4]*Please refer to Part II: Alternative Dispute Resolution of the Advisory Guidelines on Enforcement of the Data Protection Provisions.*

***Expedited Decision Procedure ("EDP"): Breach Findings with Warning, Directions and Financial Penalties***

The expedited decision procedure (EDP) process allows investigations to be completed in a significantly shorter period of time, while achieving the same enforcement outcomes. In order to avail themselves to the EDP process, an organisation will have to intimate its intention at an early stage of the PDPC's investigations, and provide the following:

1. An upfront voluntary admission of liability for breaching the relevant obligation(s) under the PDPA by the organisation and the organisation's role in the cause(s) of breach;

2. Relevant facts of the incident (this may include internal or external forensic investigation reports undertaken by the organisations and the steps taken by the organisation to mitigate the incident and to prevent recurrence etc.); and

3. Written confirmation of willingness to comply with direction(s) and/or financial penalty notice issued by the PDPC.

The PDPC will then proceed to find the organisation in breach of the PDPA based on the information provided, and in particular, the organisation's voluntary admission of liability. Save where an organisation is a repeat offender, an organisation's voluntary admission of liability, made at an early stage of the investigations through the EDP process, is a factor that the PDPC will consider favourably should a financial penalty be under consideration.

Similar to the full investigation process, the PDPC may issue a Preliminary Decision which sets out the proposed direction(s) to be issued and/or proposed financial penalty notice to be imposed. The organisation may choose to make representations with relevant supporting documents enclosed. Before issuing the Final Decision, the PDPC will consider the representations presented for the findings made in the Preliminary Decision.

The Final Decision will be published by the PDPC.

The organisation's request in writing to the PDPC to invoke the expedited decision procedure process must be made soon after the incident is known, i.e. either upon commencement of investigations and/or in the early stages of investigations. In the request, the organisation must intimate that it is prepared to admit liability to breaching the relevant obligation(s) under the PDPA in relation to the incident. Subsequently, the organisation must provide a written statement, with the following information:

1. An account of the incident with all relevant facts;
2. The causes of the incident, including all relevant technical details;
3. The relevant employees (and their supervisors) who were involved in the incident and the details of their said involvement;
4. The employees who were assigned data protection roles and their involvement in the incident;
5. The practices, policies and/or procedures which were in place during the material time of the incident in relation to the protection of personal data in the possession and/or control of the organisation;
6. Full copies of the reports of all internal and/or external investigations of the incident, if any;
7. An admission as to the acts and/or omissions that constitute a breach of the PDPA;
8. All relevant evidence supporting all material facts;
9. The relevant sections of the PDPA which the organisation has breached; and
10. All actions taken by the organisation to either remediate or mitigate the consequences of the breach.

The PDPC will review the information provided before considering whether to accept the organisation's request to invoke the expedited decision procedure process by executing a legally binding written agreement between the organisation involved and the PDPC.

The PDPC will **not** accept an organisation's request to invoke the expedited breach decision procedure process when:

1. The organisation refuses to provide an upfront voluntary admission of liability for breaching the relevant obligation(s) under the PDPA and the organisation's role in the cause(s) of breach; or

2. The organisation refuses to accept the terms and conditions of the expedited decision procedure process.

The PDPC may exercise its discretion to discontinue the expedited decision procedure process and proceed with a full investigation of the incident at any time before the conclusion of the case.

Where an organisation does not comply with the direction(s) and/or the financial penalty notice(s) issued by the PDPC upon completion of the investigation, the PDPC will take steps as it thinks fit in the circumstances to enforce the relevant compliance.

# FINANCIAL PENALTIES

# FINANCIAL PENALTIES (*SECTION 48J OF THE PDPA*)

As a matter of enforcement policy, the PDPC's approach is to first consider the nature of the breach and whether directions without financial penalties are effective in remedying the breach. Financial penalties are intended to achieve compliance and deter non-compliance. The PDPC will consider the imposition of a financial penalty when it is necessary to reflect the seriousness of the breach.

For a breach of the Data Protection Provisions, section 48J of the PDPA provides that the PDPC may impose a financial penalty of up to S$1 million or 10% of the organisation's annual turnover in Singapore[5], whichever is higher. The revised financial penalty caps takes effect on 1 October 2022.

[5]*Where the organisation's annual turnover in Singapore exceeds S$10 million.*

In determining the financial penalties to be imposed, the PDPC will employ the following approach:

1. Assess the incident based on the principles of harm and culpability, drawn from the factors set out in section 48J of the PDPA;
   (i) **Harm** includes the number of affected individuals, categories of affected personal data, duration of the incident etc. The PDPC will determine the level of harm in accordance with the above factors;
   (ii) **Culpability** refers to the organisation's conduct in the incident. The PDPC will consider the nature of the specific breach of the PDPA as well as the organisation's overall compliance with the PDPA;

2. Consider other relevant factors calling for an increase and/or decrease of the financial penalty. Such factors include, but are not limited to, the following:
   (i) Whether the organisation or person took any action to mitigate the effects and consequences of the non-compliance, and the timeliness and effectiveness of that action;
   (ii) Whether the organisation or person had previously failed to comply with the PDPA etc;
   (iii) Whether there was voluntary admission of liability, including whether done under the Expedited Decision Procedure;
   (iv) Whether there was cooperation with the PDPC during the course of the investigation;
   (v) Whether the organisation or person is a first-time offender.

3. Adjust the financial penalty by considering the likely impact on the organisation or person as well as considering if it is proportionate and effective with regard to achieving compliance and deterring non-compliance.

# ADDITIONAL RESOURCES

# ADDITIONAL RESOURCES

Organisations are encouraged to refer to the following resources on the PDPC's website, which provide more information on the areas that are mentioned briefly in this Guide.

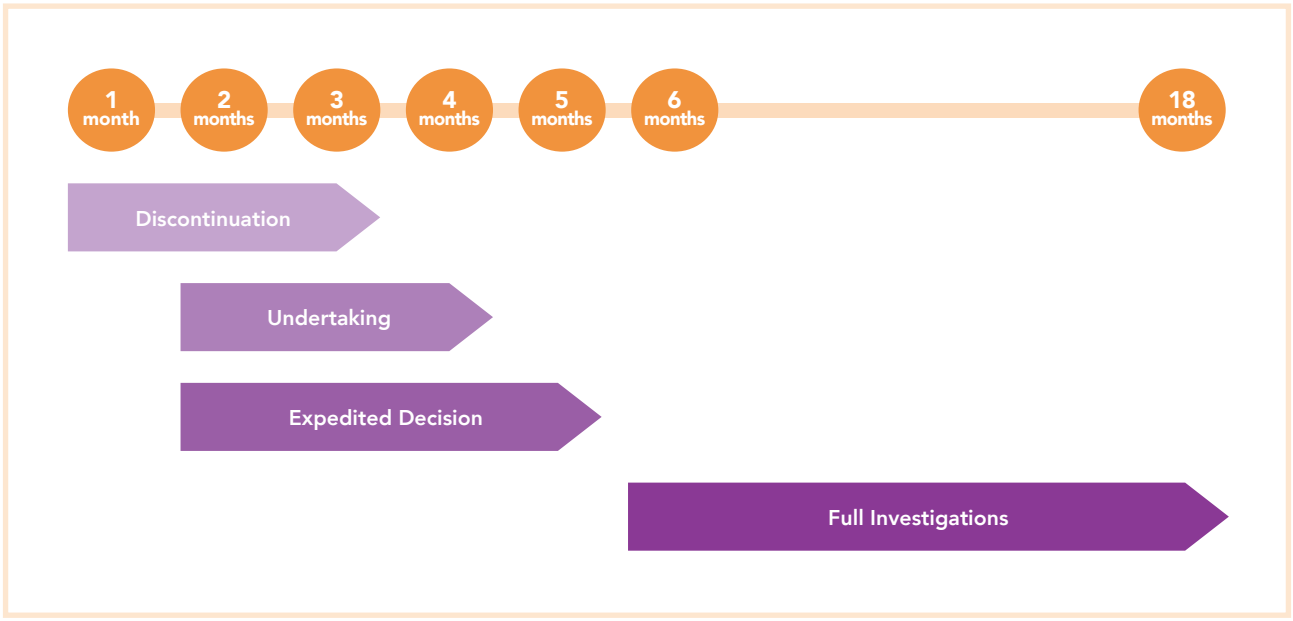
1. Advisory Guidelines on Enforcement of the Data Protection Provisions.
2. Guide on Managing and Notifying Data Breaches under the PDPA.

***Other Advisory Guidelines and Guides***

3. Advisory Guidelines on Key Concepts in the PDPA.
4. Advisory Guidelines on the PDPA for Selected Topics.
5. Advisory Guidelines on the PDPA for NRIC and other National Identification Numbers.
6. Guide to Managing Data Intermediaries.
7. Guide to Accountability under the PDPA.
8. Guide to Developing a Data Protection Management Programme.
9. Guide on Data Protection Policies for ICT Systems.

# ANNEX A: ESTIMATED TIMELINES FOR INVESTIGATION CLOSURE

Generally, the following are the estimated timelines for the closure of cases received and investigated by the PDPC. However, depending on the nature of the cases, investigations may take longer to complete.



## #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