Revised on 15 March 2021

GUIDE ON

ACTIVE ENFORCEMENT

SG:D
EMPOWERING POSSIBILITIES

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

CONTENTS

PART I: INTRODUCTION 4
Overview of Framework 5
Facilitation and Mediation 7
Goals of the PDPC Taking Enforcement Action 8

PART II: INVESTIGATION PROCESS 9
Investigation Process 10

PART III: TYPES OF ENFORCEMENT ACTIONS 11
Types of Enforcement Actions 12

PART IV: FINANCIAL PENALTIES 27
Financial Penalties (new section 48J of the PDPA) 28

PART V: ADDITIONAL RESOURCES 30
Additional Resources 30

ANNEX A: Estimated Timelines for Investigation Closure..... 31

INTRODUCTION

OVERVIEW OF FRAMEWORK

The Personal Data Protection Act 2012 ("**PDPA**") came into force on 2 July 2014. The PDPA confers enforcement powers to the Personal Data Protection Commission ("**PDPC**") to investigate and utilise enforcement powers in relation to 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 technology. When considering the appropriate enforcement action, the PDPC is guided by three key objectives:

(i) 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;

(ii) to be proportionate and consistent in the application of enforcement action on organisations that are found in breach of the PDPA; where penalties imposed serve as an effective deterrent to those that risk non-compliance with the PDPA; and

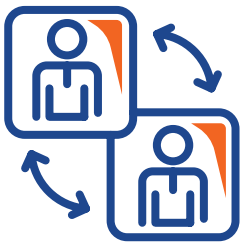
(iii) to ensure that organisations that are found in breach take proper steps to correct gaps in the protection and handling of personal data in their possession and/or control.

The changing digital landscape and the rise of data analytics in recent years have enabled many new services to consumers. Digital social platforms connect more people, electronic commerce offerings are more personal, digital services predict consumer needs better and have become more interactive. These services are driven by personal data and using them in turn generates more personal data. The proliferation of smart devices, lifestyle gadgets and smart home devices adds to the digital exhaust that consumers are creating and organisations are collecting and processing in order to make services more personalised. However, the drive for new services and better use of data also brings about higher risk of mishandling or misuse of personal data.

The scope of the PDPA is wide. Consequently, not all complaints and incidents can be investigated. Following the amendments to the PDPA which came into force on 1 February 2021, this guide on Active Enforcement Guide Framework ("**Framework**") articulates the PDPC's approach in deploying its enforcement powers to act effectively and efficiently on the increasing number of incidents. This guide targets both consumers as well as organisations that handle personal data. It also 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. Notwithstanding, the PDPC will not hesitate to send a clear message of wrongdoing where necessary. This guide will therefore outline how the PDPC handles data protection complaints, investigates incidents and the types of enforcement actions that the PDPC may undertake in various circumstances[1]. In addition, this guide will explain the general principles for determining the financial penalty amount imposed for cases where the organisations are found to be in breach of the PDPA.

This guide provides insight into the PDPC's enforcement policy but 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.

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



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 the new section 48G(1) of the PDPA. It is to be noted that where the PDPC finds facilitation and/or mediation to be inappropriate in the circumstances, 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.

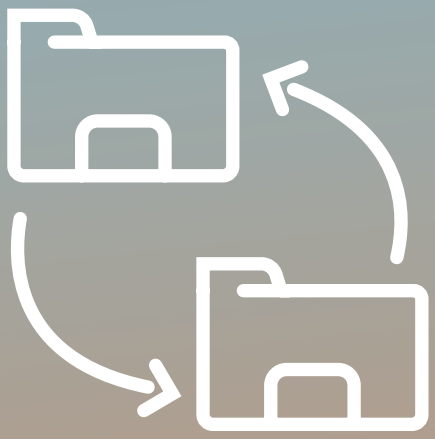
More information about how the PDPA is generally enforced and approach to resolving complaints via facilitation and mediation can be found in the Advisory Guidelines on Enforcement of the Data Protection Provisions.

GOALS OF THE PDPC TAKING ENFORCEMENT ACTION

The PDPC, in taking enforcement actions, aims to encourage organisations to be in compliance with the PDPA. Concurrently, 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 have also been published on its website. Such publications will be made at the PDPC's discretion and confidential information will be redacted. By communicating the Decisions publicly, the PDPC, as a personal data protection regulator, proposes to:

1. increase public awareness of the organisational obligations pursuant to 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 imbed 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.

With these in mind, the Framework aims to continue the provision of more 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 girds 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 actions would be further elaborated in Part III: Types of Enforcement Actions.

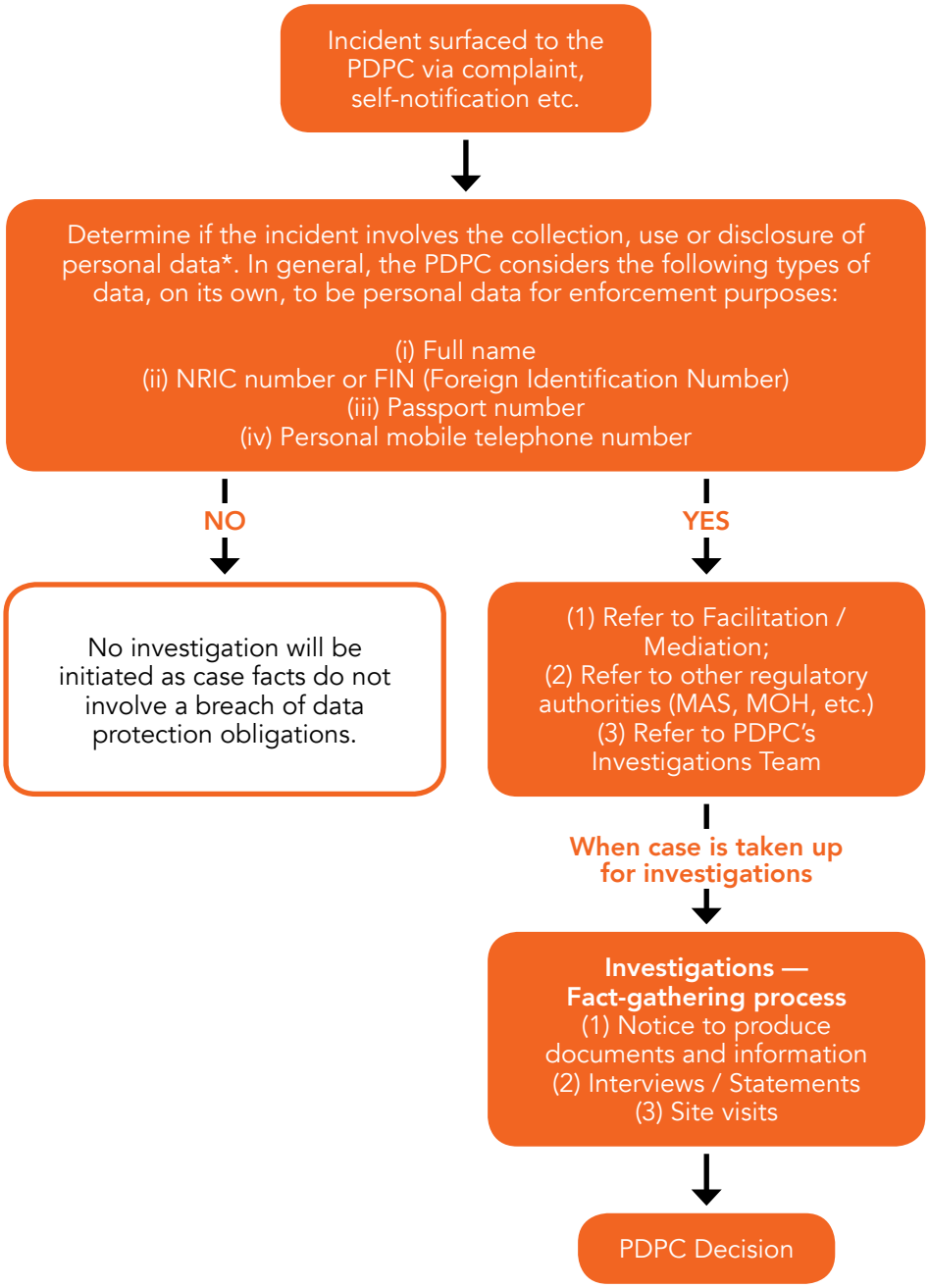


INVESTIGATION PROCESS

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 simple summary of the investigation process is shown below:



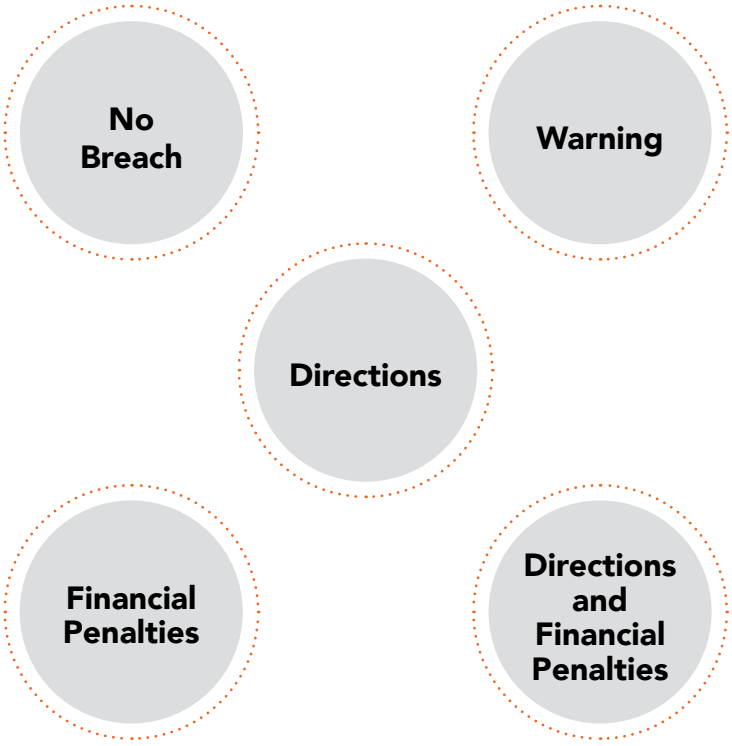
** Personal data is defined in section 2 of the PDPA to refer to data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access.*

TYPES OF ENFORCEMENT ACTIONS

TYPES OF ENFORCEMENT ACTIONS

Under the Framework, the PDPC may take the following enforcement actions on the organisations it investigates into:

1. **Suspension or discontinuation** of the investigation;
2. **Voluntary undertaking**;
3. **Expedited breach decision**;
4. **Full investigation process**, which may result in the following decisions:



SUSPENSION OR DISCONTINUATION

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 where the impact is assessed to be low. 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 the new 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 another 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 breach but serves as a tool of instruction highlighting the areas that the organisation(s) can improve on, in order to be in better compliance with the PDPA. For instance, guidance on best practices when sending out mass external emails or the pointers to strengthen personal data safeguarding efforts could be provided to the organisation(s) as part of the advisory notice.

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. This 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.

In 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.

Example:

Sending email with email addresses visible to every recipient

Retail store ABC sent email invitations to promote the launch of its new products and invite members to a members-only preview sale. Retail store ABC sent the email to 50 members but failed to insert their email addresses in the Bcc: field. Instead, the email addresses and in some instances, accompanying names, were inserted in the To: field, allowing 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 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 might 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 in 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.

In 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 might 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 date of expiration 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 to individuals was assessed to be low and the details of the other member were only disclosed to one party, i.e. Ms E, the PDPC might discontinue the investigation and issue an advisory notice to organisation HIJ.

VOLUNTARY UNDERTAKING *(NEW SECTION 48L OF THE PDPA)*[2]

Under certain circumstances, as an alternative to a full investigation, the PDPC may accept a written voluntary undertaking from the organisation. The voluntary undertaking process is intended to allow organisations with demonstrable accountability practices (for example an organisation which is IMDA Data Protection Trustmark certified, has effective monitoring and breach management systems etc.) and an effective remediation plan to be given the opportunity to implement their remediation plan in relation to the incident within a specified time.

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 possibility of a voluntary undertaking may arise when:

1. the organisation is able to demonstrate that it has in place accountable policies and practices;

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

The organisation's request in writing to the PDPC to invoke the voluntary undertaking process must be made very soon after the incident is known, i.e. either upon commencement of investigations and/or in the early stages of investigations. The request must be accompanied with a remediation plan and should state how the requirements enumerated in Points (1) and (2) above 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.

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

The voluntary undertaking will take effect upon acceptance by the PDPC in writing of the organisation's duly executed undertaking. A voluntary undertaking does not amount to a finding of a data breach.

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, if such publication or publicity is one of the terms of the voluntary undertaking, e.g. organisation publishing the relevant part of its undertaking or publicising its commitment to provide affected individuals with free security monitoring service for a limited period.

The voluntary undertaking will typically, at a minimum:

1. be signed by the Chief Executive Officer of the organisation or another authorised senior management officer;
2. describe the incident that the organisation is involved in;
3. 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
4. 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 PDPC is **unlikely** to accept a voluntary undertaking request in any of, but not limited to, the below scenarios:

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;

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

4. the organisation requests for extended time to produce a remediation plan; or

5. the breach is wilful or egregious.

Where an organisation withdraws its request for the voluntary undertaking option before submitting the written voluntary undertaking or the PDPC's acceptance of the same, the PDPC may proceed with a full investigation of the incident and/or impose any other enforcement action 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, including imposing available enforcement remedies under the PDPA pursuant to section 50(3A). The PDPC may still publicise the voluntary undertaking and a full investigation of the incident may be conducted. The PDPC may also give directions to comply with the voluntary undertaking pursuant to new section 48L(4).

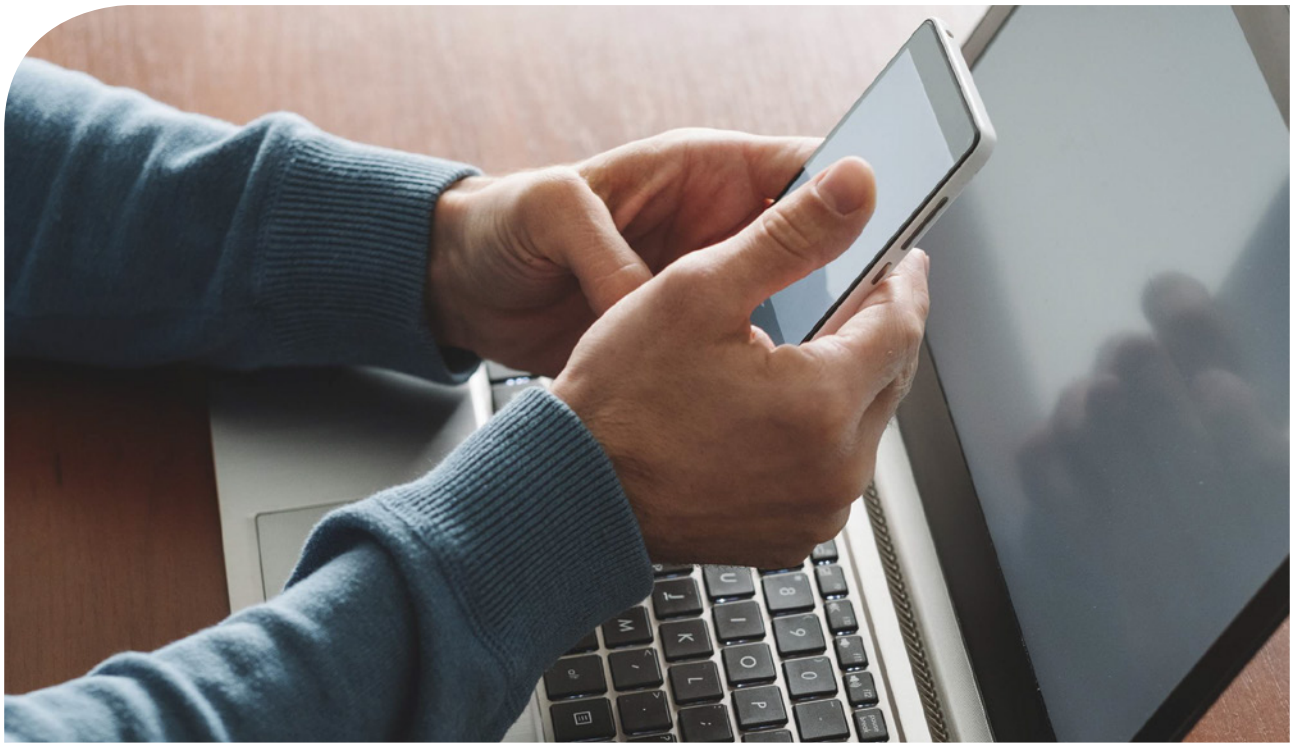
Example:

Where the organisation requests 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 purposes 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 plans to introduce a two-factor authentication, halt the practice of shared login credentials to the administrative account, make its administrative account more secure, improve its alert system to detect possible intrusions, amongst others. 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.



EXPEDITED BREACH DECISION

Under certain circumstances, an expedited breach decision may be considered by the PDPC. The expedited breach decision process allows investigations to be completed in a significantly shorter period of time, while achieving the same enforcement outcomes. The process entails:

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. provision of the relevant facts of the incident by the organisation (this may include steps taken to mitigate the incident and to prevent recurrence etc); and

3. compliance with the relevant direction(s) issued by the PDPC.

Accordingly, there will be a finding of breach of the PDPA by the organisation in an expedited breach decision.

Upon completion of the expedited breach decision process, the PDPC will issue a Decision and set out the relevant direction(s) that the organisation is required to comply with, including any financial penalties. Where financial penalties are involved, the organisation's admission of its role in the incident could be taken as a mitigating factor. However, admissions are unlikely to be a strong mitigating factor for repeated data breaches.

The expedited breach decision will be published by the PDPC.

In general, the PDPC will consider accepting a request to invoke the expedited breach decision process in the following situations:

1. when the only breach of the PDPA by the organisation(s) involved is that it has **no Data Protection Officer ("DPO") or equivalent and/or no Privacy Policy**; or

2. when the nature of the data breach is **similar to precedent cases with similar categories of facts**. Examples include:
   (a) **insecure direct object reference vulnerability**: The most common example is URL manipulation where the parameters in the URL string can be changed to gain unauthorised access to separate web-subpages disclosing personal data;

   (b) **poor governance in relation to the use of IT**: Examples include personal data disclosed via email through loose controls and redundant web-connected accounts with administrative level access;

   (c) **poor password policy and/or weak password management**: Examples include poor enforcement of password strength requirements, password sharing and no password renewal;

   (d) **occurrence of printing and/or enveloping errors**: Examples include personal data disclosed due to weak controls in printing or enveloping processes, poor processes for the disposal of unwanted documents with personal data;

   (e) **inadequate knowledge of organisation's IT system or features**: Examples include failure to discover the correct security settings when employing open source or off-the-shelf software and IT forms (e.g. Google Forms), and failure to put in place reasonable access controls to servers, directories and files; and

   (f) **ransomware incidents**: Examples include personal data encrypted by ransomware attacks. Personal data should not have been exfiltrated and incident did not involve high data loss of impacted data.

The organisation's request in writing to the PDPC to invoke the expedited breach decision process must be made very 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 indicate 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 breach decision 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 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;

2. the incident did not qualify in one of the situations as listed in Points (1) and (2)(a) to (f) on page 22; or

3. the organisation refuses to accept the terms and conditions of the expedited breach decision process.

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

Where an organisation does not comply with the direction(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.

Example:

Poor password policy and/or weak password management

The database of company MNO had been subjected to an alleged incident. The suspected perpetrator had accessed the database and posted the personal data of approximately 10,000 individuals on a public online forum. The personal data comprised names, national identification numbers and bank account details.

In the course of investigations, company MNO requested for the investigations to be placed on the expedited breach decision process. It also readily admitted to the PDPC that it had a poor password policy in place and it did not conduct regular security testing at the material time. This made it easy for the suspected perpetrator to gain access to the database.

As the cause of the breach is very similar to precedent cases, the PDPC is likely to consider accepting company MNO's request and will issue an expedited Decision based on the precedent cases. This may include directions and/or Financial Penalty.

Example:

Occurrence of printing and/or enveloping errors

Company PQR prints letters in-house and sends them via mail to its customers. Such letters typically comprise the names, national identity numbers, residential addresses and contact numbers. In this incident, one of company PQR's employees had failed to follow the SOP and it resulted in an enveloping error. While performing the enveloping, the employee did not verify whether all the documents matched the same customer and inserted the wrong letters in the envelopes.

In the course of investigations, company PQR requested for the investigations to be placed on the expedited breach decision process. Company PQR readily admitted to the PDPC that it did not enforce the SOP strictly and could have reminded its employees on a more regular basis to ensure that the SOP had been followed.

As the cause of the breach is very similar to precedent cases, the PDPC is likely to consider accepting company PQR's request and will issue an expedited Decision based on the precedent cases. This may include directions and/or Financial Penalty.

Example:

Did not have processes in place to ensure relevant settings in IT systems were configured to restrict access of personal data to only authorised parties

Company STU possesses a customer database meant for its internal sales employees to access. The settings were originally set for access to authorised employees only. However, as part of a routine database maintenance exercise, a newly employed IT employee accidentally altered the settings from private to public, thereby allowing the public to gain access to the internal customer database.

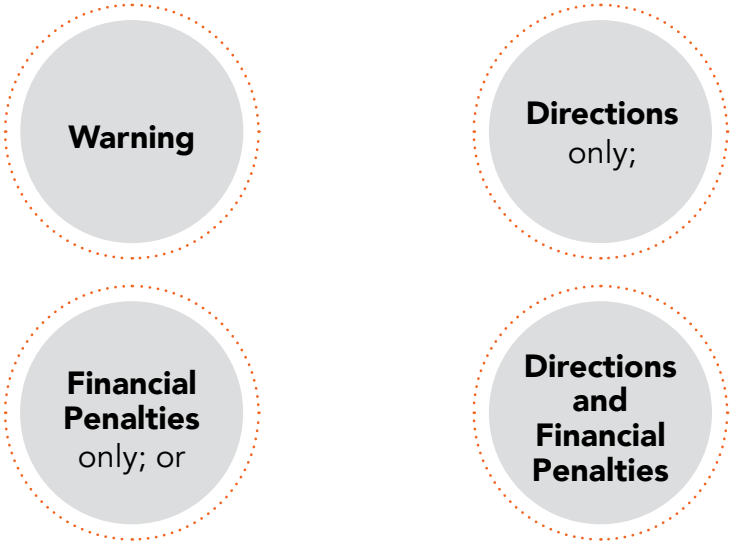
In the course of investigations, company STU requested for the investigations to be placed on the expedited breach decision process and readily admitted to the PDPC that it did not ensure sufficient oversight on the IT employee tasked with the maintenance exercise. There was also no robust SOP in place to make sure that a senior officer checks and signs off on the maintenance exercise. Consequently, this increased the chances of the settings not being set correctly after the exercise.

As the cause of the breach is very similar to precedent cases, the PDPC is likely to consider accepting company STU's request and will issue an expedited Decision based on the precedent cases. This may include directions and/or Financial Penalty.

FULL INVESTIGATION PROCESS

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 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 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 actions may be imposed on the organisation:



More details on the investigation process are available in the Advisory Guidelines on Enforcement of the Data Protection Provisions.

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

FINANCIAL PENALTIES

FINANCIAL PENALTIES (NEW SECTION 48J OF THE PDPA)

As a matter of enforcement policy, the PDPC's approach is first to consider the nature of the breach and whether directions without financial penalties are effective in remedying the breach. Financial penalties are intended to act as a form of sanction and deterrence against non-compliance when directions alone do not sufficiently reflect the seriousness of the breach. In considering whether to direct an organisation to pay a financial penalty, the PDPC will take into account the seriousness of the incident of the breach.

For a breach of the Data Protection Provisions, the new 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 are to take effect no earlier than 1 February 2022.

In calibrating the financial penalties, the PDPC considers the specific circumstances and the conduct of the organisation in each case. As set out in the new section 48J(6) of the PDPA, these include, but are not limited to, the following factors:

1. **the nature, gravity and duration** of the non-compliance by the organisation;
2. the **type and nature of the personal data** affected by the non-compliance by the organisation;
3. whether the organisation, as a result of the non-compliance, **gained** any financial benefit or **avoided** any financial loss;
4. whether the organisation took any action to **mitigate** the effects and consequences of the non-compliance, and the **timeliness and effectiveness** of that action;
5. whether the organisation, despite the non-compliance, **implemented adequate and appropriate measures** for compliance with the requirements under the PDPA;
6. whether the organisation had **previously failed** to comply with the PDPA;

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

7. the compliance of the organisation with any previous direction issued by the PDPC;

8. whether the financial penalty to be imposed is **proportionate and effective**, having regard to achieving compliance and deterring non-compliance with the PDPA;

9. the **likely impact** of the imposition of the financial penalty on the organisation, including the ability of the organisation to continue the usual activities of the organisation; or

10. any other matter that may be relevant, for example, voluntary notification of the data breach

Please refer to Table 1: Factors and examples of past enforcement cases in Part VI: Directions to Secure Compliance (Written Notice to pay financial penalties) of the Advisory Guidelines on Enforcement of the Data Protection Provisions for examples of how these considerations have been applied in past cases.

Notwithstanding the new higher financial penalty cap in the PDPA, the PDPC will continue to calibrate financial penalties in a manner that is **proportionate** to the seriousness of the contravention and provide **sufficient deterrence** against future or continued non-compliance. That said, where the PDPC determines that a contravention is particularly egregious by the facts of the case and circumstances, the PDPC may consider imposing a substantially higher financial penalty to achieve the desired enforcement outcome.

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.

ADVISORY GUIDELINES

Organisations may refer to the PDPC's website at **www.pdpc.gov.sg/ag** for related advisory guidelines:

1. Advisory Guidelines on Enforcement of the Data Protection Provisions.
2. Advisory Guidelines on Key Concepts in the PDPA.
3. Advisory Guidelines on the PDPA for Selected Topics.

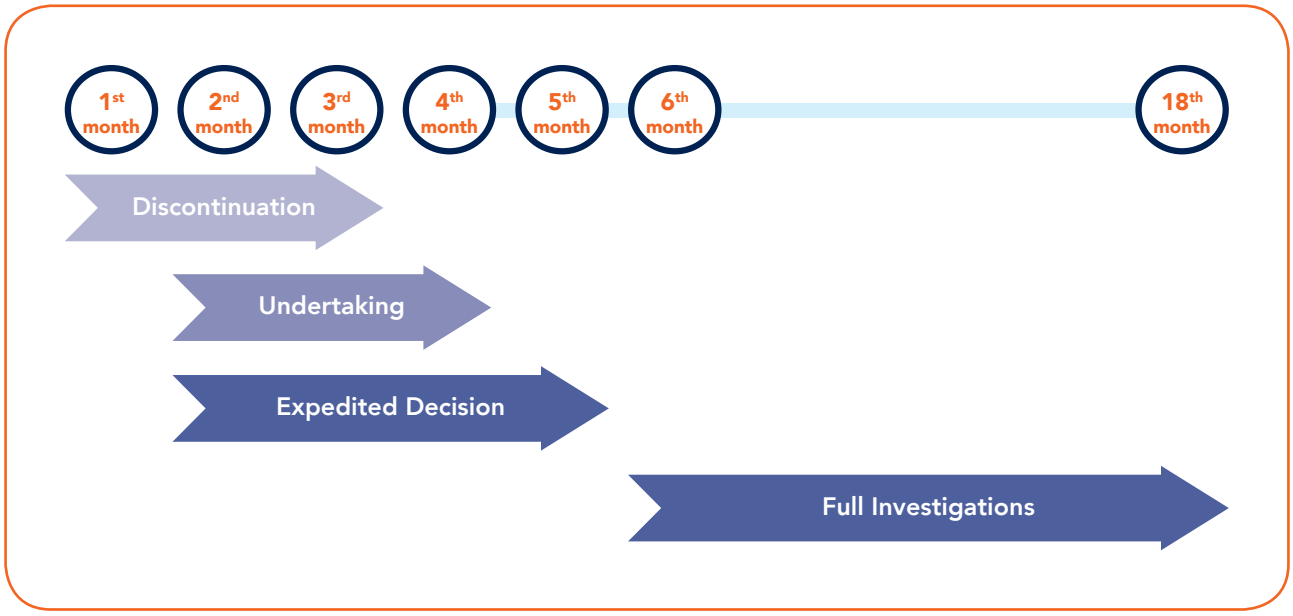
OTHER GUIDES

Organisations may also refer to the PDPC's website for other useful guides:

1. Guide on Managing and Notifying Data Breaches under the PDPA.
2. Guide to Accountability under the PDPA.

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