INTRODUCTION ................................................................................................... 4
Overview of Framework ......................................................................................... 5
Facilitation And Mediation ..................................................................................... 6
Goals of the PDPC Taking Enforcement Action ..................................................... 7

INVESTIGATION PROCESS ................................................................................. 8

TYPES OF ENFORCEMENT ACTIONS .............................................................. 10

FINANCIAL PENALTIES ....................................................................................... 27

ADDITIONAL RESOURCES .................................................................................. 29

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.

The PDPC’s objective 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. When considering whether to take enforcement action, the PDPC is guided by the 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 harm or loss 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 to the PDPA.
(iii) To ensure that organisations that are found in breach take proper steps to correct gaps in the protection of personal data.

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 add 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 bring 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. This guide on the Active Enforcement Framework ("Framework") articulates the PDPC’s new 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. 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.

**FACILITATION AND MEDIATION**

The PDPC recognises that personal data protection issues often 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, with the consent of both the complainant and the organisation, refer the matter for mediation, pursuant to section 27(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 investigation early. Such cases may involve disclosure of personal data on a large scale and/or involve data of a more sensitive nature.

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.

---

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.
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 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 promote the positive behaviours that the PDPC would like to see in organisations with respect to their handling of personal data and related incidents. Subject to the PDPC’s discretion and criteria, the PDPC may decide to apply enforcement options that reflect the responsible conduct that the organisations exhibit.
INVESTIGATION PROCESS
Details about the investigations 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:
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. **Undertaking**
3. **Expeditied Decision**
4. **Full investigation process**, which may result in the following decisions:
   - **No Breach**
   - **Warning**
   - **Directions**
   - **Financial Penalties**
   - **Directions and Financial Penalties**
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 section 27(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; or
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 will 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 compliant 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 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 Ms A may be posted on its notice boards. This action serves to inform its employees/patrons of the presence of an unauthorised individual. Consequently, organisation CDE grabbed a screenshot of Ms A via its CCTV footage and posted on notice boards within its premise.

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

In this case, there are ongoing legal proceedings involving Ms A and organisation CDE relating to the incident. Hence, the PDPC is likely to 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 on salon XYZ’s official social media platform.

The screenshots contained their IM exchanges which contained details of the package. 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 to respond to the latter’s posting on the social media platform. In this case, as the organisation had not disclosed Ms B’s personal data, Ms B’s complaint would be regarded as frivolous or vexatious, and the PDPC is likely to discontinue the investigation.
Example:

Sending email with email addresses visible to every recipient

To promote the new launch of retail products, retail store ABC decided to send out a mass email introducing the products and inviting members to a Members-Only preview sale. It 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 names to be made privy to all recipients of that Email. A member of the retail store, Ms C, lodged a complaint with the PDPC, alleging that the retail store had used and disclosed her personal data without her consent.

Retail store ABC admitted that a procedural lapse caused the breach and it was well aware that the email addresses should have been inserted in the Bcc: field. It had sent out an apology email to affected members. As the impact of the breach was assessed to be low and the email addresses and/or names 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 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 informed about being in compliance with the PDPA and the staff should not have created the Group without the consent of its registered job-seekers. Company EFG had promptly deleted the Group and sent out 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 disclosed to 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, the organisation decided to send her an email about membership renewal.

However, as the process was done manually, the organisation inserted the details of another member in the email meant for Ms E. The details of the other member comprised name, mobile number, membership number and date of expiration of the membership. 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 details to her without consent.

Organisation HIJ admitted that it was a human error and that it will enhance its system to ensure that no such incident happens again. Organisation HIJ had 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.
UNDERTAKING

Under certain circumstances, the PDPC and/or the organisation may initiate an undertaking process. The acceptance of an undertaking is solely within the PDPC’s discretion. The PDPC may consider accepting such a request from the organisation under certain circumstances. The undertaking process includes a written agreement between the organisation(s) involved and the PDPC in which the organisation(s) voluntarily commits to remedy the breaches and take steps to prevent recurrence. The undertaking process is intended to allow organisations with good accountability practices and an effective remediation plan to be provided with a window of opportunity to implement their remediation plans. A key consideration is the effectiveness of the remediation plan and the organisation’s readiness to implement it forthwith.

The organisation’s request to invoke the 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; and the organisation will not be given additional time to produce the remediation plan. Accountability requires that organisations are ready with drawer plans (e.g. data management plans comprising remediation processes, incident responses procedures) to deal with foreseeable incidents. One of the goals of undertaking is to allow accountable organisations to implement such drawer plans. The terms of any undertaking will typically, at a minimum:

1. be signed by the Chief Executive Officer of the organisation or an equivalent rank;
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 rectify the cause of the incident. Such measures should include steps to reduce recurrence of the incident as well as putting in place monitoring and reporting processes, audits and policy/process reviews;
4. include the provision of a person responsible for overseeing compliance of the undertaking and reporting to the PDPC;
5. contain the organisation’s acknowledgement to provide related reports of the third party to the PDPC if and when requested for;
provide the steps to be taken for affected individuals to be notified of the incident and steps that can be taken to reduce risk of harm or loss to the individual;

provide a channel or hotline for affected individuals to find out more about the incident;

outline any steps the organisation will take to resolve a data protection disputes arising with affected individuals; and

provide the organisation’s agreement for the undertaking to be published in full by the PDPC. (The PDPC will consider redacting matters that are commercially confidential.)

The possibility of an undertaking may arise when:

• the organisation is able to demonstrate that it has in place accountable practices, for example a Data Protection Trustmark certified organisation, and is ready to implement its remediation plan; or
• the PDPC is of the view that an undertaking achieves a similar or better enforcement outcome more effectively and efficiently than a full investigation.

The PDPC will not accept an undertaking request when:

• the organisation refutes responsibility for the data breach incident; 
• the undertaking does not explain how the compliance may be achieved; 
• the organisation requests for time to produce a remediation plan; 
• the organisation refuses to accept the undertaking terms and conditions; 
• the organisation seeks to impose terms and conditions on the PDPC, beyond those relating to confidentiality of information; or 
• the organisation does not agree for the undertaking to be published

The PDPC will work together with the organisation(s) involved to pinpoint areas of improvement, specifically in relation to the incident. In this manner, the organisation’s data protection awareness can be heightened as well.
Example:

Where the organisation agrees to undertake, 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. The company admitted to the PDPC that the incident might have occurred due to a shared administrative account to its database.

Company GHI was forthright in its admission and was quick to remedy the incident. It introduced 2FA and halted the practice of shared login credentials to the administrative account. Company GHI also had a remediation plan which included changes to make its administrative account more secure and a more robust alert system to detect possible intrusions, amongst others. Company GHI is also Trustmark certified by the IMDA for two years and had intimated to the PDPC that it was willing to undertake implementation of its remediation plan.

In this case, company GHI had been Trustmark certified for a reasonable period, and was cooperative. There was also a remediation plan put in place by company GHI to ensure that the direct cause(s) of breach had been addressed and other measures introduced to enhance the security of its IT system. Therefore, the PDPC is likely to consider offering the undertaking option to company GHI.
EXPEDITED BREACH DECISION

An expedited decision may be considered by the PDPC at its discretion in certain circumstances and there is an upfront admission of liability for breaching relevant obligation(s) under the PDPA by the organisation(s) involved on its/their role in the cause of breach. The expedited decision allows investigations to be completed in a shorter period of time, yet achieving the same enforcement outcome in a full investigation.

Where financial penalties are involved, the organisation’s admission of its role in the incident will be taken as a strong mitigating factor. However, admissions might not be considered as a mitigating factor for repeated data breaches.

Expedited decisions are intended to reduce the time and resources required for investigations significantly, partly through the voluntary admission of the relevant facts and the organisation’s role in the case of breach. The PDPC will still issue a full decision even if it is expedited and will set out the relevant direction(s) that the organisation(s) is required to comply with, including any financial penalties.

Organisations that are considered for expedited decisions must make a written request to the PDPC when investigations commence. Each organisation must also intimate that it is prepared to admit liability to the relevant obligation(s) under the PDPA in relation to the data breach incident. It will provide and admit to all relevant information of the incident as well as identify the areas to which it is admitting liability to. Upon receipt of the above, the PDPC will review the information provided before deciding on the request.
In general, PDPC will consider having an expedited decision 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 are:

   (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) Failure to acquire knowledge of security of the 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.
Example:

**Poor password policy and/or weak password management**

The database of company MNO had been subjected to alleged data breach incident. The alleged 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 admitted to the PDPC that it had a poor password policy in place and did not conduct regular security testing at the material time. This made it easy for the alleged perpetrator to gain access to the database.

As the cause of the breach is very similar to precedent cases, the PDPC 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 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 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 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 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 directly. The PDPC has an established facilitation and mediation process to encourage DPOs and complainants to resolve the matter amicably. However, for incidents with 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(s) is determined by the PDPC, the following enforcement actions may be imposed on the organisation(s):

- **Warning**
- **Directions only**
- **Financial Penalties only**
- **Directions and Financial Penalties**


---

FINANCIAL PENALTIES
FINANCIAL PENALTIES

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. Generally, financial penalties are reserved only for breaches which the PDPC views as particularly serious in nature.

In assessing the seriousness of the breach, the PDPC considers a number of factors, including but not limited to the following:

1. **Impact** of the organisation’s breach.
2. Whether the organisation had **acted deliberately or wilfully**.
3. Whether the organisation had **known or ought to have known** the risk of a serious contravention and **failed** to take reasonable steps to prevent it.
4. **Extent of non-compliance** in terms of the PDPA obligations that the organisation had failed to discharge.
5. **Number of individuals** whose personal data had been subjected to **harm and risks** as a result of the breach.
6. Whether the organisation had appointed a **DPO or equivalent** to ensure accountability with the PDPA.
7. **Types of personal data** that were compromised or put at risk as a result of the breach.
8. Whether the organisation had **previously** been found to have similarly breached the PDPA.
The PDPC determines each case on its own merits and circumstances. However, the PDPC adopts an objective approach to assess the seriousness of a breach of the Data Protection Provisions of the PDPA, by considering how a reasonable organisation should behave in a particular situation. Where a financial penalty is warranted, the PDPC adopts the following principles to determine the amount:

1. The amount should be proportionate to the seriousness of the breach.
2. The amount should provide sufficient deterrence against future or continued non-compliance by the organisation and others.
3. The amount should take into account aggravating and mitigating factors.
4. Cooperativeness of the organisation in the course of investigations.
5. Whether remedial action(s) were implemented.
6. Whether there was voluntary notification of the data breach.
7. Whether the organisation had engaged with the affected individuals in a meaningful manner and had voluntarily offered a remedy, and that the individuals had accepted the remedy.
8. Whether the organisation admitted to liability for the data breach.
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:

2. Advisory Guidelines on Key Concepts in the PDPA
3. Advisory Guidelines on the Personal Data Protection Act for Selected Topics

OTHER GUIDES

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

1. Guide to Managing Data Breaches 2.0
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.
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.