GUIDE TO ACCOUNTABILITY UNDER THE PERSONAL DATA PROTECTION ACT

SG:D
EMPOWERING POSSIBILITIES

pdpc
PERSONAL DATA PROTECTION COMMISSION SINGAPORE

CONTENTS

THE NEED FOR ACCOUNTABILITY IN A DIGITAL ECONOMY 4

ACCOUNTABILITY PRINCIPLE 6

ACCOUNTABILITY WITHIN AN ORGANISATION 8

ACCOUNTABILITY WITHIN INDUSTRY 15

ACCOUNTABILITY IN ENFORCEMENT 17

ANNEX 19

THE NEED FOR ACCOUNTABILITY IN A DIGITAL ECONOMY

Organisations today operate in an increasingly connected and competitive digital economy where individuals' online and real-world activities generate a burgeoning amount of data.

In such a competitive and evolving business environment, a "check-box" compliance approach towards the handling of personal data is increasingly impractical and insufficient to keep pace with the developments in data processing activities.[1] Organisations that focus on compliance through such an approach may find themselves disadvantaged and unable to use data for innovation.

Over time, with greater awareness of the risks surrounding the unauthorised collection, use and disclosure of personal data, consumers are increasingly cautious about how organisations are using and managing personal data, and place greater value on trust and accountability.

It is thus important for organisations to shift from a compliance-based approach to an accountability-based approach in managing personal data. This helps organisations strengthen trust with the public, enhance business competitiveness and provide greater assurance to their customers, all of which are necessary factors for organisations to thrive in the digital economy.

This guide explains the accountability principle in the context of personal data protection and how organisations may demonstrate accountability for personal data in their care. The accountability practices highlighted in this guide are not meant to be exhaustive. Organisations should assess what tools and resources would be appropriate for use in their specific circumstances.

[1] *For example, through the growth in volume and complexity of data processing arising from the use of Artificial Intelligence, sensor networks or the Internet of Things.*

ACCOUNTABILITY PRINCIPLE

Accountability in relation to personal data protection is the undertaking and demonstration of responsibility for the personal data in the organisation's possession or control. As a principle in personal data protection frameworks, accountability was first introduced in 1980[2] by the OECD and has since gained traction internationally. For example, accountability is one of the key principles[3] highlighted under the APEC Privacy Framework. Accountability is also one of the obligations in the European Union General Data Protection Regulation ("**GDPR**").[4]

Accountability is a fundamental principle of the Personal Data Protection Act ("**PDPA**"),[5] which requires organisations to ensure and demonstrate compliance with the PDPA. Collectively, sections 11 and 12 of the PDPA form the accountability obligation under the PDPA. First and foremost, an organisation is responsible for the personal data in its possession or under its control. Each organisation is required to:

a. develop and implement policies for data protection;

b. communicate and inform their staff about these policies; and

c. implement processes and practices that are necessary to meet their obligations under the PDPA.

Additionally, organisations are to make information about its data protection policies and practices available to consumers. Finally, data protection officers are appointed to be responsible for ensuring that organisations are in compliance with the PDPA.[6]

Besides having the capacity to comply with legal requirements, an accountable organisation should be able to demonstrate proper management and protection of personal data. This includes adapting legal requirements into policies and practices, utilising monitoring mechanisms and controls to ensure that polices and processes are effectively implemented and inculcating an organisational culture of responsibility through training and awareness programmes.

Above all, an accountable organisation is answerable to regulatory authorities[7] and individuals who entrust the organisation with personal data, such as its customers, employees as well as business partners seeking to engage the organisation to process personal data.

[2] *In the Organisation for Economic Cooperation and Development's ("OECD") Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. As originally articulated, accountability was a principle that focused on establishing who had responsibility for compliance with data protection principles.*

[3] *Published in 2005, the accountability principle under the Asia-Pacific Economic Cooperation ("APEC") Privacy Framework placed responsibility on the data controller to be accountable for ensuring that the recipient will protect the personal data, and take reasonable steps to ensure that data protection obligations were met after the transfer of personal data. In addition, the Enhanced Data Stewardship Accountability Elements by the Information Accountability Foundation ("IAF") introduces additional elements for organisations such as the "ethics by design" process and the Ethical Data Impact Assessment ("EDIA").*

[4] *The EU GDPR, which came into effect in May 2018, integrates accountability by requiring organisations to put in place and demonstrate appropriate accountability measures in Article 5 and 24 of the EU GDPR.*

[5] *This principle pre-dates the PDPA and its roots may be traced to the 2003 voluntary Model Data Protection Code for the Private Sector. Accessible here.*

[6] *For more information, refer to the PDPC's Advisory Guidelines on Key Concepts in the Personal Data (The Accountability Obligation).*

[7] *Including the PDPC as well as any other relevant sectoral regulatory authorities.*

ACCOUNTABILITY WITHIN AN ORGANISATION

While there are mandatory accountability requirements under the PDPA, organisations should consider accountability measures beyond merely complying with the law. As good practice, organisations could consider demonstrating accountability in the areas of Policy, People and Process.[8]

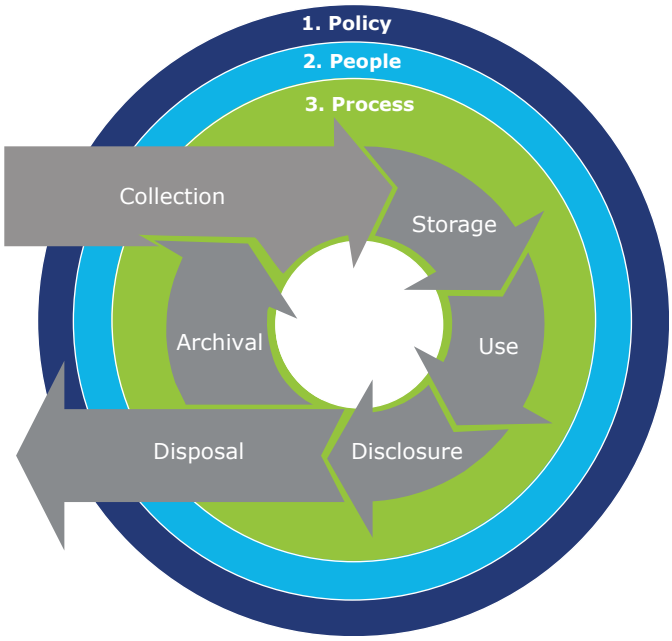


Diagram of Policy, People, Process within a data lifecycle (From Collection to Archival/ Disposal)

Policy

Good accountability practices begin with an organisation's leadership, and is directed through its corporate governance and policies. A key step to ensure a commitment to accountability is to embed personal data protection into corporate governance[9] as the involvement of the senior management is crucial.

Responsibilities of senior management include the following:

a. Appointing a Data Protection Officer ("**DPO**"),[10] preferably from senior management,[11] who can effectively direct and oversee data protection initiatives. The DPO will be supported by representatives from various organisational functions.

[8] *"Policy, People and Process" is a framework that organisations may also use to develop a Data Protection Management Programme. For more information, organisations may refer to the PDPC's Guide to Developing a Data Protection Management Programme ("DPMP Guide").*

[9] *This includes having data protection as an aspect of compliance and IT risks so that data protection gets attention at the Board-level, and that data protection risks are included in Enterprise Risk Management Frameworks.*

[10] *The PDPA requires organisations to designate at least one individual to be the DPO responsible for ensuring that the organisation complies with the PDPA.*

[11] *In the DPMP Guide, the PDPC expects senior management to oversee the following activities: appointing the DPO; approving the organisation's data protection policies and DPMP; monitoring and managing personal data protection risks as part of corporate governance (e.g. corporate risk management framework), and where relevant, reporting to the Board which typically oversees risk governance; commissioning Data Protection Impact Assessments ("DPIAs"); advocating data protection training; allocating resources (e.g. budget, manpower) to data protection; providing strategic guidance on the implementation of data protection initiatives; providing direction to DPO for the handling of major complaints; and providing direction to DPO for communication and liaison with the PDPC.*

b. Endorsing the organisation's data protection management programme that is developed to address and suit the business needs of the organisation.

c. Monitoring and managing personal data protection risks by establishing an enterprise risk management framework with effective reporting mechanisms (i.e. regular risk reporting and internal audit) that addresses personal data protection issues.

d. Communicating the organisation's approach to handling personal data throughout the organisation.

With the tone set by the senior management, an organisation's personal data protection policies[12] will chart how the organisation and its staff treat personal data and its approach to managing data protection risks. These personal data protection policies should be developed and communicated to both internal stakeholders (e.g. staff), and external parties (e.g. customers). Having dedicated internal policies on specific areas will also provide clarity to internal stakeholders on the responsibilities and processes on handling personal data in their day-to-day work.

Example

Recognising the importance of an accountability-based approach to personal data protection, the senior management of Organisation ABC sets out to embed personal data protection as part of its corporate governance framework. It develops and puts in place a reporting mechanism to manage personal data protection risks through an enterprise risk management framework. It also appoints Thomas, a member of the senior management, as ABC's DPO to drive and oversee data protection initiatives.

As a DPO, Thomas sets up and oversees a team to handle ABC's data protection initiatives, including developing a Data Protection Management Programme ("**DPMP**"). Thomas ensures that the DPMP is endorsed by the senior management. He approves all internal circulars on data protection matters, instead of delegating the decision-making responsibility to junior staff.

[12] *The DPMP Guide provides general guiding questions to help organisations develop their data protection policies to suit their business or organisational needs. The PDPC has also developed a Data Protection Notice Generator to generate basic data protection template notices to inform their stakeholders on how they manage personal data. In addition, the PDPC's Self-Assessment Tool for Organisations ("PATO") is a quick and easy way for an organisation to conduct a high-level self-evaluation to identify areas for improvement when it comes to personal data protection.*

People

Personal data protection is the responsibility of every employee, and not only limited to appointed data protection representatives of the organisation. It cuts across roles, functions and hierarchy and should be practised by staff (including volunteers and contract staff) at all levels of the organisation as well as third-party service providers.

As part of corporate governance, it is important for an organisation to ensure that its staff are aware of and adheres to its data protection policies and processes. As such, it is key for an organisation to communicate its data protection policies and educate its staff on their responsibilities. One practical approach would be to embed data protection-related topics as part of staff training and development throughout the employment journey.

A structured training and communications plan is critical to effectively equip staff with the necessary knowledge and resources to manage personal data. In order to develop the right corporate culture towards data protection, the plan should take into consideration the frequency, target audience and mechanisms to ensure awareness of data protection policies and practices (e.g. mandatory tests). In addition, staff who handle personal data and those with added responsibilities, such as the appointed DPO, should receive in-depth training customised to their areas of responsibility.[13]

It is also important for personal data protection policies and processes to be clearly documented and easily accessible to staff for reference (e.g. on the organisation's intranet).

[13] *In this regard, organisations may refer to the PDPC's DPO Competency Framework and Training Roadmap to enable working professionals to acquire the relevant skills and know-how to fulfil the role and responsibilities of a Data Protection Officer.*

Example

As part of ABC's corporate governance, ABC's DPO, Thomas, and his team develop a personal data protection communications and training plan to better foster a culture of data protection in ABC.

The plan takes into account the employment journey of ABC's staff, including senior management as well as its engagements with third-party service providers.

For instance, the plan includes on-boarding orientation on data protection policies, on-the-job training on data protection processes and ongoing reminders to ensure awareness of data protection responsibilities.

Besides incorporating the communications and training plan as part of the staff's employment journey, Thomas and his team ensures that ABC's data protection policies are easily accessible through ABC's intranet for staff to refer to at any time.

Processes

An accountable organisation not only develops and communicates its data protection policies, but also puts in place effective processes to operationalise its data protection policies throughout the data lifecycle (i.e. from collection to disposal of personal data) and across business processes, systems, products or services.

To set up specific processes, an organisation should begin by documenting its personal data flows to understand how personal data is being collected, stored, used, disclosed and archived/disposed. Thereafter, it should identify key gaps and areas for improvement with respect to data protection, before incorporating data protection practices into business processes, systems, products or services.

For example, organisations may wish to implement a DPMP to operationalise their data protection policies.[14] Organisations should also implement processes for Data Protection Impact Assessments ("**DPIA**")[15] to be carried out to identify and address personal data protection risks. In addition, organisations could consider adopting the Data Protection by Design ("**DPbD**") approach when designing and building information and communications technology ("**ICT**") systems.[16]

Apart from day-to-day operational processes, organisations could also demonstrate accountability by establishing an enterprise risk management framework with monitoring and reporting mechanisms as part of managing personal data protection risks, and conducting regular reviews on data protection practices. It would also allow organisations to identify potential weaknesses and take steps or put in place remedial measures to mitigate personal data protection risks identified.[17]

On the whole, an organisation's set of processes should be reviewed on a regular basis to ensure that it meets the organisation's business needs, and is up-to-date with regulatory and technological developments.

[14] *Refer to the DPMP Guide for suggested in designing processes to operationalise policies.*

[15] *The PDPC's Guide to Data Protection Impact Assessment introduces and outline key principles and considerations for conducting a DPIA. By completing a DPIA, an organisation would be better positioned to identify risks on personal data protection and the means by which to address them. As good practice, DPIAs should be conducted regularly instead of as a one-off exercise.*

[16] *The PDPC's Guide to Data Protection by Design for ICT Systems aims to assist organisations that wish to apply DPbD when designing and building ICT systems. DPbD is an approach where data protection measures are considered and built into ICT systems that involve the processing of personal data as they are being developed.*

[17] *Organisations may refer to the Board Risk Committee Guide ("BRC") Guide developed by the Singapore Institute of Directors for more information on the board's oversight role of ensuring the adequacy and effectiveness of a company's risk management and internal controls within the context of the business and regulatory environment in Singapore.*

Example

Organisation ABC recognises that data breaches often lead to financial losses and a loss of consumer trust for the organisation. Thomas, its DPO, and his team establishes a process to address and manage complaints, disputes and personal data breaches. Such a proactive approach helps to demonstrate ABC's commitment to accountability and build trust with consumers.

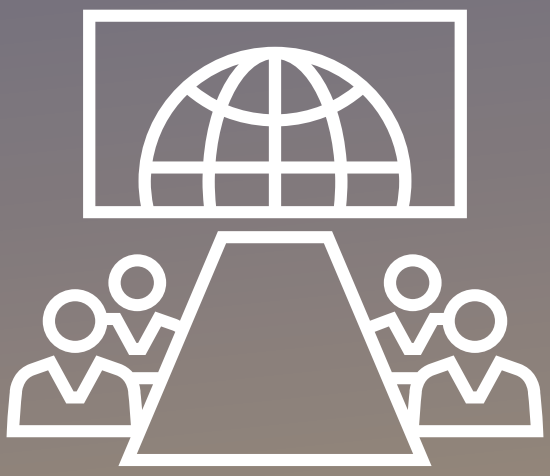
In developing a data breach management plan,[18] Thomas considers ABC's business operations and personal data flows. Key elements of the plan include setting out how data incidents[19] are to be reported within ABC, how ABC will respond to data breaches and the roles and responsibilities of the data breach management team. It also includes operational details such as steps on how to assess data incidents, reduce impact of a data breaches, remediate harm to affected individuals, and procedures for notifying affected individuals, the PDPC and other relevant regulatory authorities.

To ensure that the data breach management plan is robust, Thomas organises simulation exercises within ABC to test out key elements of the plan. While each data breach response needs to be tailored to the circumstances of the incident, contingency plans developed and refined following these simulation exercises help to better prepare ABC for possible data breaches and enable ABC to respond to them in a prompt and effective manner.

Accountability Tools

To provide practical assistance and help organisations put accountability into practice, the PDPC has developed and promoted the adoption of accountability tools, such as the DPMP, risk and impact assessments (e.g. DPIA) and gap analysis assessments (e.g. PATO) for organisations. A summary of these resources, in the form of guides, online assessments, and customisable templates can be found in the **Annex**.

[18] *The PDPC's Guide to Managing Data Breaches 2.0 aims to help organisations develop data breach management plans and how it can better manage a data breach.*
[19] *Data incidents refer to a potential, but unconfirmed breach, of the Protection Obligation under the PDPA.*



ACCOUNTABILITY WITHIN INDUSTRY

Accountability practices have enabled the development and implementation of a number of initiatives to support commerce between or with accountable organisations.

Organisations may choose to engage an independent third party assessor to certify their data protection policies and practices through the Data Protection Trustmark ("**DPTM**") Certification.[20] The DPTM certification helps provide greater assurance to customers and business partners on the accountable policies and practices that the organisation has put in place to safeguard their personal data. The DPTM certification provides an additional option to organisations who require business partners or suppliers to adhere to an independently verified standard in their data protection practices, for example when procuring services that handle large volumes of personal data.

Singapore is also a participant of the APEC Cross Border Privacy Rules ("**CBPR**") and Privacy Recognition for Processors ("**PRP**") Systems, which comprise a set of APEC-approved requirements to demonstrate compliance and accountability. Organisations certified under the APEC CPBR and/or PRP Systems must meet these requirements and will be recognised by other participating APEC economies. The APEC CBPR and PRP Systems establish a network of accountable organisations in participating APEC economies in order to facilitate the cross border flow of data between them in support of cross border trade.

[20] *It is a voluntary enterprise-wide certification that help organisations demonstrate accountable and responsible data protection practices.*

ACCOUNTABILITY IN ENFORCEMENT

The PDPC's Active Enforcement Framework[21] builds upon the principles of accountability in promoting positive behaviours by organisations when handling personal data and related incidents. In certain circumstances, the PDPC may apply enforcement options that take into consideration the accountable conduct of the organisation. Under the Active Enforcement Framework, in the event of a data incident, organisations with accountable practices may consider the option of (a) an undertaking and/or (b) expedited enforcement decision, instead of a full investigation, under certain circumstances specified by the PDPC.

An organisation that has detected a data incident early and demonstrated that it has established processes to respond to it quickly and effectively may submit to the PDPC an undertaking to voluntarily commit to implement its remediation plan and resolve the breach. This is applicable to organisations that have good accountability practices (e.g. the organisation has attained certification under the Data Protection Trustmark).

An expedited enforcement decision may be given by the PDPC if an organisation makes an upfront admission of liability for breaching relevant obligation(s) under the PDPA. The voluntary admission of the organisation's role in the breach will be taken as a strong mitigating factor where financial penalties are involved. The option provides accountable organisations an opportunity to conduct themselves in a dignified manner.

[21] *For more information, please refer to the Guide on Active Enforcement on the PDPC's approach to enforcement.*

ANNEX

The PDPC has developed and made available on the its website various resources to guide organisations in building a robust personal data protection infrastructure. As there is no one-size-fits-all solution to personal data protection, each organisation will need to assess the appropriate measures and tools that are suited to its business needs and circumstances.

The PDPC will continue to support the development of accountable data protection practices within organisations to facilitate data innovation in Singapore's Digital Economy.

Tool	Description
Developed by the PDPC	
PDPA Assessment Tool for Organisations (PATO)	Organisations seeking to identify any gaps in policies or processes when it comes to personal data protection can use PATO to conduct a high-level self-evaluation of their personal data protection policies. From there, organisations would be able to find other appropriate resources that best meet their business needs.
Data Protection Starter Kit	The Data Protection Starter Kit contains useful information and resources such as sample forms, clauses and communication materials that organisations can adopt to kick-start the implementation of their data protection management programme.
Guide to Developing a Data Protection Management Program (DPMP)	This guide provides a systematic framework to help organisations establish a robust personal data protection infrastructure. It highlights key considerations for organisations in setting out their management policies and processes for the handling of personal data and in defining the roles and responsibilities within the organisation in relation to personal data protection.
Guide to Data Protection Impact Assessments (DPIA)	This guide aims to introduce and outline key principles and considerations for conducting a DPIA, a process that seeks to identify, assess and address personal data protection risks. It describes the roles and responsibilities of stakeholders and highlights that DPIAs should be conducted in line with the organisation's policies or project management practices. The Guide also includes examples to illustrate how certain steps within the DPIA process may be undertaken. By undertaking a DPIA, an organisation would be better positioned to identify risks on personal data protection and the means by which to address them.
Guide to Managing Data Breaches 2.0	This guide aims to help organisations develop data breach management plans and provide considerations for organisations when formulating their framework for managing and minimising data breaches, including reporting to the PDPC.

Tool	Description
Guide to Data Protection by Design for ICT Systems	This guide aims to assist organisations that wish to apply DPbD when designing and building ICT systems. DPbD is an approach where data protection measures are considered and built into ICT systems that involve the processing of personal data as they are being developed. It is intended for IT project managers, system architects and software developers involved in system or software development work. DPOs will gain a better understanding of how good practices fit into the system development process. This guide provides information on: • DPbD principles; • DPbD activities in each phase of the Software Development Lifecycle; (**"SDLC"**); and • Good data protection practices for ICT systems.
Guide on Active Enforcement	This guide aims to provide information on PDPC's approach to enforcement, which encompasses a new expedited decision process, enhanced undertaking process, and a greater emphasis on the facilitation and mediation process.
Data Protection Notice Generator	The Data Protection Notice Generator seeks to help organisations generate basic data protection template notices to inform their organisation's stakeholders (e.g. customers, employees, job applicants and donors, service users and volunteers) on how they are managing their personal data.
Corporate e-Learning Programme	The Corporate e-Learning Programme helps organisations to equip their employees with the essentials of the PDPA as well as evaluate their understanding through the assessment module.
DPO Competency Framework and Training Roadmap	The framework provides guidance for organisations to build capabilities in data protection and build consumer trust and confidence when safeguarding their personal data. The framework is designed to provide greater clarity of the competencies required for Data Protection Professionals to perform their roles more effectively.
Other Resources	Other resources available for organisations on the PDPC's website include advertisements, e-newsletters, videos, posters and electronic direct mailers to promote awareness of the PDPA, brochures, handbooks and leaflets to provide concise information in bite-sized formats, and sample clauses and templates to enable organisations to demonstrate accountability.
Developed by industry	
Personal Data Asset Inventory Tool (Docukit Data Protection App)	The Docukit Data Protection App helps DPOs track how personal data is being managed within their organisations, and therefore manage the data protection risks in a more effective and productive manner.
DPOinBox	The DPOinBox supports organisations in the development and implementation of their data protection management programme for areas such as identifying risks, managing the programme, sustaining initiatives and responding to incidents and requests.

#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