GUIDE TO
DATA PROTECTION BY DESIGN
FOR ICT SYSTEMS

PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

CONTENTS

INTRODUCTION

OVERVIEW OF DATA PROTECTION BY DESIGN

Data Protection by Design ("**DPbD**") for information and communications technology ("**ICT**") systems 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. By taking into consideration data protection principles from the start, organisations will be able to build systems to better safeguard personal data and create a culture of good data management practices. Ensuring DPbD at the onset and throughout the lifecycle of an ICT system also helps to reduce unnecessary delays and contain costs, compared to having to retrofit data protection features afterwards. DPbD should not be an afterthought but instead, be embedded into organisations' practices.
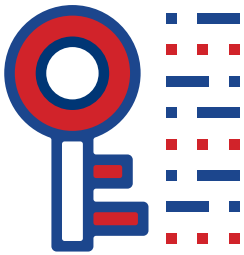
PURPOSE OF THIS GUIDE

This Guide aims to assist organisations that wish to apply DPbD when designing and building ICT systems. It is intended for IT project managers, system architects and software developers involved in system or software development work. Data Protection Officers ("**DPOs**") will gain a better understanding of how good practices fit into the system development processes. 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.

Note that the tips and good practices listed in this Guide are not exhaustive and may not be relevant for all situations. Each organisation should therefore adopt practices that are reasonable and appropriate for their business and operational circumstances.

DATA PROTECTION BY DESIGN PRINCIPLES

The seven foundational principles[1] of Privacy by Design developed by Dr Ann Cavoukian, former Information and Privacy Commissioner of Ontario, are well recognised and often referred to by many data protection experts.

Referencing the seven foundational principles, the seven DPbD principles which are relevant and important in guiding the development of ICT systems are as follows:

1 **Proactive and preventive**
Assess, identify, manage and prevent any data protection risks before data breaches occur. Risks can be minimised through good design and data management practices.

2 **Data protection as the default**
Data protection measures must be integrated into processes and features of the systems. Individuals should not have to take actions for their personal data to be protected, and measures to safeguard personal data should be automatically provided as default settings.

3 **End-to-end security**
Security measures must be considered in the complete SDLC. Good security features and practices can be incorporated at every stage of the SDLC, and from the point that personal data is collected until it is purged from the system.

Users should also consider "end-to-end" in terms of how their organisations and vendors work together, as well as how the components of their ICT system – the software, hardware, products, services and platforms – work together.

Look out for any vulnerable parts from this "end-to-end" perspective and assess how to strengthen security.

[1] https://www.ipc.on.ca/wp-content/uploads/resources/7foundational principles.pdf

4 **Data minimisation**

Do not be tempted to adopt a "collect first and think of what to do with it later" approach when it comes to personal data. Data minimisation means to strictly collect, store and use personal data that is relevant and necessary for the intended purpose for which data is processed.

5 **User-centric**

Develop and implement ICT systems with individuals in mind – specifically, with the goal of protecting their personal data. Do this through default settings while giving individuals the option to customise settings with informative notices. The interface must be user-friendly, and features such as "just-in-time" notification or layered notices can be applied.

6 **Transparency**

Take an active role in informing individuals on what personal data is collected from them and how it is being used. Also inform users of any third parties processing their personal data. Identify and use the most appropriate means to provide such information, which could be at different points of interaction with the individual or through "just-in-time" notices.

7 **Risk minimisation**

An important aspect of DPbD is to systematically identify and mitigate data protection risk. Risk can be reduced by designing and implementing the right processes and relevant ICT security measures when processing personal data.

DATA PROTECTION BY DESIGN AND THE SDLC

The following table summarises the main activities that take place at the various SDLC phases.

SDLC Phase	DPbD Activity
Requirements	This is where DPbD begins. Assess and identify requirements that do not have a clear purpose or are unreasonable from a data protection perspective. Such requirements can be removed.
Design	This is a crucial phase to ensure that DPbD principles are incorporated into the design at the system architectural level.
Development	This phase is where the system is being developed, and the DPbD principles are considered and then incorporated into the various components, functions and features.
Testing	This phase is where checks are performed to ensure that the requirements and DPbD considerations defined in the earlier phases have been validated by test results.
Deployment	This phase is where the system is being prepared for release. A final check on the processes and system configuration is conducted before the release.
Maintenance	This phase is where the system needs to be kept secure and post-deployment system enhancements are made. DPbD considerations need to be continually applied here as the organisation reviews and updates its systems.

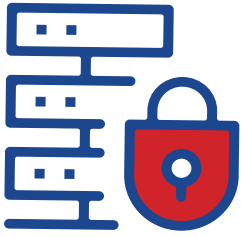# DATA PROTECTION BY DESIGN AND AGILE SOFTWARE DEVELOPMENT

The software development model described in the previous section is commonly referred to as the "waterfall" model. In the waterfall model, all requirements for the system are made known upfront and addressed collectively, going through one iteration of the SDLC, sequentially and largely linearly.

Agile software development is another approach to software development. Compared to the waterfall approach, the agile development approach develops systems in an incremental and iterative manner, addressing bits of requirements at each iteration, over many iterations.

As each Agile iteration is still similar to the relevant parts of the waterfall SDLC, the good practices suggested in this Guide remain applicable to the Agile development model.

In practice, there is probably more flexibility and less cost to implement fundamental design features and changes from the start. Hence, it would be more cost-effective for DPbD features to be considered and planned for, even if not immediately constructed, during the initial iteration where possible.

In terms of data protection impact assessments ("**DPIA**"), it is recommended to perform a comprehensive DPIA at the beginning of the Agile project with as much information available as possible. Thereafter, the DPIA assessment can be updated during the subsequent iterations or where relevant to repeat the DPIA exercise.

DATA PROTECTION BY DESIGN FOR EXISTING ICT SYSTEMS

It is ideal to build in DPbD to new ICT systems. In reality, organisations are likely to have at least some existing ICT systems. What, then, can organisations do to improve data protection for such existing ICT systems?

Associate Professor Marilyn Prosch and Dr Ann Cavoukian developed the concept of "Privacy by Redesign"[2] for existing ICT systems. The three "Rs" of the concept are:

Rethink

Rethink includes thoroughly reviewing the existing system, considering what personal data is being collected and whether the collection is completely necessary, assessing risk, etc. Hence, it is suitable to conduct a DPIA at this 'rethink' stage.

Redesign

Redesign involves implementing relevant DPbD good practices to better protect personal data and reduce the risks identified earlier.

Revive

Revive refers to starting afresh with the data protection-enhanced system.

Organisations may decide to implement the re-engineering process at one go, or incrementally over multiple phases.

---

[2] http://www.ontla.on.ca/library/repository/mon/25005/310082.pdf

GOOD DATA PROTECTION BY DESIGN PRACTICES FOR ICT SYSTEMS

GOOD PRACTICES

This section presents a list of good DPbD practices for ICT systems. The good practices are organised by topics. Users should select relevant good practices to adopt or adapt accordingly for their ICT projects. Note that the list of good practices is not exhaustive.

To assist software developers in knowing where to apply the good practices, the suggested association of each good practice with the most relevant phase(s) of the SDLC, as well as to the relevant tier(s) in the commonly used "3-tier" architecture (presentation, application and data tiers[4]) is indicated with a 'tick' symbol. The associations of the good practices to the SDLC and tiers are not meant to be prescriptive.

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

DPIAs may be conducted at any point in time during the SDLC, but from a DPbD perspective, a good time to conduct them is when the preliminary design of a new ICT system has been established.

Good Practices	SDLC Phase						Tier		
	Requirements	Design	Development	Testing	Deployment	Maintenance	Presentation	Application	Data
1. Conduct DPIA before development Critically assess the types of personal data and the data processing activities required for achieving the purposes of the new ICT system. This helps to identify and assess the gaps and risks in the design of the new ICT system, in terms of personal data. The preliminary design of the ICT system may then be modified and mitigating measures may be incorporated, if necessary, to address the gaps and risks identified. For more information, refer to the PDPC's *Guide to Data Protection Impact Assessments.*	✓	✓				✓			

---

[4] The presentation tier is responsible for presentation of information and user interaction, the application layer manages the business logic of the application, while the data layer is where the data is stored and managed.
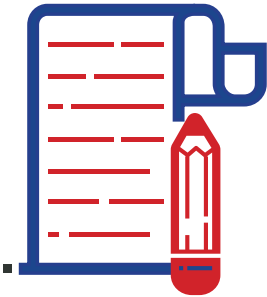
COLLECTION OF PERSONAL DATA BY ICT SYSTEMS

Personal data that is collected but not used only burdens organisations with unnecessary risks. The resources that would have been needed to protect these "unnecessary personal data" can be avoided simply by not collecting them in the first place. Therefore, a good way to begin is to think about what personal data one's organisation really needs.

Good Practices	SDLC Phase						Tier		
	Requirements	Design	Development	Testing	Deployment	Maintenance	Presentation	Application	Data
1. Minimise collection of personal data Do not collect personal data unless it will be used, and there is a valid purpose for doing it. For each data field, ensure that the collection is: • for a lawful and reasonable purpose that is directly related to a function or activity of the organisation; and • not excessive for the purpose. When different types of personal data are used to achieve the same purpose, collect the least sensitive types of personal data (e.g. collect approximate location data of users rather than their exact locations).	✔	✔				✔	✔	✔	
2. Only collect information on personal identifiers (e.g. national identification number) when absolutely necessary These tend to be unique values that directly identify persons. Hence, extra consideration should be given as to whether there is a need to collect. In the Singapore context, only collect NRIC numbers if required under the law or when necessary to accurately establish or verify the identity of the individual to a high degree of fidelity. For more information, refer to PDPC's *Advisory Guidelines on the Personal Data Protection Act for NRIC and Other National Identification Numbers*.	✔	✔				✔	✔	✔	

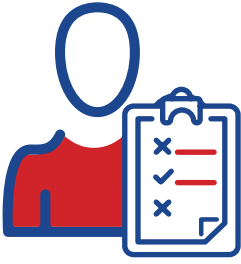| Good Practices	SDLC Phase						Tier		
	Requirements	Design	Development	Testing	Deployment	Maintenance	Presentation	Application	Data
3. Beware of metadata Personal data may be unknowingly collected in the form of metadata (e.g. EXIF data in image files). Consider not collecting such data or removing them if they are not needed.	✓	✓				✓		✓	✓
4. Collect personal data only when needed instead of continuously For example, in a mobile app, provide the option for the user to indicate his/her location only at the point in time when this location information is really needed rather than collecting location information all the time.	✓	✓	✓			✓	✓	✓	
5. Collect personal data through user input instead of automatically obtaining it Some users may prefer convenience but others may prefer less intrusion. For example, in a mobile app, provide the user with the option to indicate his/her location, instead of automatically obtaining the location from location tracking.	✓	✓	✓			✓	✓	✓	

NOTIFICATION OF PURPOSE & DATA PROTECTION POLICY

Organisations are required to notify individuals of the purposes and obtain their consent for collecting, using and disclosing their personal data, unless any exception applies.

Increasingly, users expect organisations to be accountable not only in the usage and protection of their personal data, but also in conveying the purpose(s) of data collection, use, disclosure, etc, as well as their data protection policies, in a way that is easy to understand. Providing clear and concise notifications is one way to put one's organisation ahead of others.

Good Practices	SDLC Phase						Tier		
	Requirements	Design	Development	Testing	Deployment	Maintenance	Presentation	Application	Data
1. Explain purpose of collection This applies especially when it may not be obvious to the user why certain information about them is being collected. Clearly indicate whether the collection of each piece of personal data is mandatory. If it is, explain the consequences of users not providing the information.		✓	✓			✓	✓		
2. List personal data collected This means the 'what' and 'how' related to personal data collected, where applicable. Examples include geolocation data collected through GPS, or Wi-Fi access points.		✓	✓			✓	✓		
3. List third parties List out third parties involved in processing the personal data (if any), what personal data is passed to the third parties, as well as the purpose.		✓	✓			✓	✓		
4. List contact information of DPO List the DPO's contact details prominently, for users to get in touch if they have queries on data protection matters.		✓	✓			✓	✓		

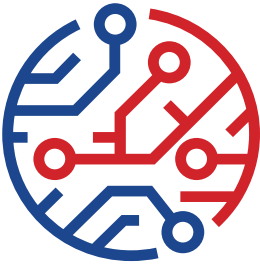| Good Practices	SDLC Phase						Tier		
	Requirements	Design	Development	Testing	Deployment	Maintenance	Presentation	Application	Data
5. Keep it simple Keep the organisation's data protection policy statement concise and readable. Doing this will increase the likelihood of it being read.		✓	✓			✓	✓		
6. Do not simply copy other's data protection policy statements When one refers to other organisations' privacy policy statements while drafting his/her own, he/she should adapt the statement as required to meet the organisation's unique needs. This may mean adding completely new elements and removing irrelevant ones.		✓	✓			✓	✓		
7. Take a layered approach If there is too much information to be communicated in the data protection policy statement, consider presenting an overview first and allowing the user to choose which sections to view in greater detail.	✓	✓	✓			✓	✓		
8. Adopt a just-in-time approach Another approach to prevent information overload is the "just-in-time" or dynamic approach (i.e. to notify just before certain personal data is collected or certain permission is required). A short version can first be presented, with an option for the user to view the full version if desired.	✓	✓	✓			✓	✓		
9. Use infographics Instead of being presented as large chunks of text, some aspects of data protection policy notices can be shown as infographics.		✓	✓			✓	✓		

GETTING CONSENT FOR USERS' PERSONAL DATA

Getting users' consent to use their personal data is something that an ICT system can help achieve very effectively. On top of that, ICT can help organisations manage consent and easily check against the consent records.

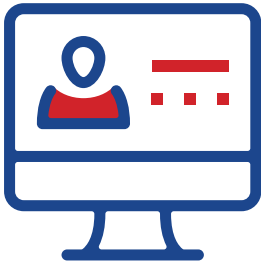| Good Practices	SDLC Phase						Tier		
	Requirements	Design	Development	Testing	Deployment	Maintenance	Presentation	Application	Data
1. Explain clearly what the user is consenting to Use simple and concise language as much as possible. If the text is lengthy, consider presenting an overview first and providing the user with the option to view more details.		✅	✅	✅		✅	✅		
2. Require explicit action for the user to indicate consent instead of establishing a default action Ensure that user has to perform an explicit action to indicate consent, e.g. the user needs to tick a checkbox and the checkbox should not be pre-ticked (i.e. automatically selected by default).		✅	✅			✅	✅		
3. Ask separately for consent to receive marketing materials If the user will be asked for consent to receive marketing materials, ask for it separately from the consent to collect personal data, e.g. via a second checkbox.		✅	✅			✅	✅		
4. Keep records of what users consented Users may consent to certain elements but not others. Therefore, it is important to keep records of what users have consented to and when these were obtained. This is sometimes referred to as a consent register.	✅	✅	✅			✅	✅	✅	

Good Practices	SDLC Phase						Tier		
	Requirements	Design	Development	Testing	Deployment	Maintenance	Presentation	Application	Data
5. Keep copies of consent messages The exact text message used by an organisation to obtain consent may change over time. Yet, these text messages are often not archived in a systematic way. Find a suitable way to keep copies of the different versions, and the date that each version started to take effect – this allows easy checking of the exact message used during a certain date and time. This could be achieved using version control software, for example. Such records can be useful in the event of disputes with users.		✔	✔			✔	✔		
6. Allow users to withdraw their consent Provide a means for users to withdraw their consent. This could be implemented through a manual process (e.g. manual processing of withdrawal request sent by email), or using a more automated way. Do note that it is likely to be easier to reflect consent withdrawal in audit trails when using automated methods. It is useful to inform users of the consequences of withdrawing their consent (if any). It is also useful for organisations to notify users on the status of their request to withdraw consent.	✔	✔	✔			✔	✔	✔	

DEVELOPMENT OF ICT SYSTEM

One of the major decisions facing organisations before embarking on an ICT project is whether to develop a new solution or to use an existing one. Depending on the approach chosen, there are different things to look out for.

Good Practices	SDLC Phase						Tier		
	Requirements	Design	Development	Testing	Deployment	Maintenance	Presentation	Application	Data
1. Spell out security requirements to ICT vendors When developing bespoke solutions through ICT vendors, one should spell out the organisation's data protection and security requirements to the vendor. Ensure that these are documented as part of the scope of work, and that they are fulfilled.	✓	✓	✓	✓	✓	✓	✓	✓	✓
2. Understand ready-made solutions before using them When intending to use ready-made solutions – whether purchased or open source – understand what the solution does to the personal data entrusted to it. One should only proceed to use the solution if his/her organisation is satisfied that personal data is adequately protected. When selecting ready-made solutions or components, consider if they are well supported by the developers. Software that are no longer supported may contain vulnerabilities that can never be patched, and therefore, be permanently vulnerable.	✓			✓		✓			
3. Apply patches Test and apply updates and security patches to relevant components of the ICT system as soon as possible. Some form of monitoring (automated or manual) is likely needed for this to be done in a timely manner.			✓		✓	✓	✓	✓	✓

ONLINE FORMS

This section is relevant to all web applications that accept any form of user input. Common threats include malicious file uploads, cross-site scripting ("**XSS**"), SQL injection and URL manipulation.

Please refer to the chapter on "Websites and Web Application Security" in the PDPC's *Guide to Securing Personal Data in the Electronic Medium* for more information.

Good Practices	SDLC Phase						Tier		
	Requirements	Design	Development	Testing	Deployment	Maintenance	Presentation	Application	Data
1. Use HTTPS instead of HTTP HTTPS is the secured, encrypted form of HTTP transmission. HTTP (the non-secure version) transmits an organisation's data in plain form, unencrypted, making it easy for personal data to be retrieved from intercepted network traffic.	✓	✓			✓	✓		✓	
2. Implement measures against the OWASP Top 10 Most Critical Web Application Security Risks[5] This list explains the most common and critical security risks in web applications, such as injection, misconfiguration, cross-site scripting and using components with vulnerabilities. It also provides suggestions on how to prevent these risks. For instance, to prevent SQL injection, some of the methods suggested are: query parameterisation, encoding, character encoding, character escaping and input validation. *The OWASP Top Ten Proactive Controls[6] is a separate but related document focussing on defensive techniques and controls. Each of the controls discussed defends against one or more items under the top ten risks.*	✓	✓	✓	✓		✓		✓	
3. Use a Web Application Firewall ("WAF") WAFs are meant to defend against typical web application attacks such as SQL injection and cross-site scripting. Hence, they can act as another layer of security in addition to those measures implemented at the application code level.	✓	✓				✓			

---

[5] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
[6] https://www.owasp.org/index.php/OWASP_Proactive_Controls

Good Practices	SDLC Phase						Tier		
	Requirements	Design	Development	Testing	Deployment	Maintenance	Presentation	Application	Data
4. Scan user uploaded files for malware Users may upload files containing malware, whether knowingly or unknowingly. Ensure that such files are free from malware before doing anything else with them.	✓	✓	✓		✓	✓		✓	
5. Validate user inputs Besides ensuring data entered by the user is valid, data validation can also prevent security issues such as URL manipulation, SQL injection and buffer overflow attacks.	✓	✓	✓			✓		✓	
6. Encrypt data at rest Encrypt personal data to provide additional security. Some ways to encrypt data at rest are to: • encrypt at the database (transparent to application); and • encrypt at the application before storing data in the database. Decryption at the application is required after retrieving from the database. Key management is an important aspect for effective encryption. Also, review the method of encryption (e.g. algorithm and key length) periodically to ensure that it is recognised by the industry as relevant and secure.	✓	✓	✓		✓	✓		✓	✓

Good Practices	SDLC Phase						Tier		
	Requirements	Design	Development	Testing	Deployment	Maintenance	Presentation	Application	Data
7. Segregate personal data that needs more protection and protect accordingly Consider segregating personal data that requires more protection to provide adequate security. Examples of providing additional protection to the segregated data are to: • give access only to a smaller, select group of users (i.e. based on the "need to know" basis) • adopt a higher degree of monitoring, alerts, audit trails, auditing, etc. • implement more stringent password requirements (e.g. longer passwords, more frequent password changes, etc). For relational databases, one way of segregation is "horizontal segregation" – that is, segregating data by database records or rows. Another way is "vertical segregation" by database fields or columns. Segregating by storing in different databases may offer stronger protection, and an alternative would be through different tables in the same database. Such segregation may be more effective when the amount of sensitive personal data is a minority compared to the entire volume of data.	✓	✓	✓			✓		✓	✓
8. Use information from free text fields carefully Be aware that it is always possible for users to enter personal data in free text form fields, and personal data in such form may not difficult to detect even with data validation.			✓			✓		✓	

ACCESS CONTROL

Should a user requesting access to personal data be granted the access? How can one's organisation ensure that only authenticated and authorised users are allowed to access the requested information? The good practices in this section help to address these questions.

For more information, refer to the section on "Authentication, Authorisation and Passwords" in PDPC's *Guide to Securing Personal Data in Electronic Medium.*

Good Practices	SDLC Phase						Tier		
	Requirements	Design	Development	Testing	Deployment	Maintenance	Presentation	Application	Data
1. Know where personal data is stored and how it flows One cannot protect something without knowing where it is. Besides the database, personal data may be found in temporary files, generated reports, files generated for communicating with other ICT systems, backups, etc. This is part of the system design, and the system architect/ system specifications should be able to provide useful information. For more information on data inventories and DPIAs, refer to the earlier sections in this guide.	✅	✅				✅			✅
2. Implement access control at the application Access control, a security technique, is a fundamental way to protect personal data. It often refers to authentication (verifying the identity of the user) and authorisation (verifying if a user has the rights to access the resource being requested). Use suitable means of access controls. This often depends on where the personal data is stored. For example, personal data accessed through the application is often stored at the database. In this situation, access control is often implemented via the application. Organisations can consider making access control to personal data to be more granular, e.g. by having only some attributes of a record being accessible to a user role and other attributes only accessible to another user role.	✅	✅	✅			✅		✅	

Good Practices	SDLC Phase						Tier		
	Requirements	Design	Development	Testing	Deployment	Maintenance	Presentation	Application	Data
3. Avoid creating backdoors that bypass access control This refers to alternative ways to use the application and access personal data without going through the access controls in place. Organisations sometimes create backdoors for testing or temporary purposes. Unfortunately, backdoors are great news for hackers, especially when organisations forget to remove them promptly. Besides hackers, search engines can also find their way in, resulting personal data being made easily accessible to Internet users.			✓		✓	✓		✓	
4. Configure access control at other parts of ICT system too Besides the application, proper access control should also be implemented at the web server, database and file systems, and other parts of the ICT system. For instance, a file placed at the web server could, depending on configuration settings, become available to Internet access (by anyone), even if the link to the file is not published and even if the website or web application does not link to it. Note that usage of the robots exclusion protocol (robots.txt) on its own does not guarantee that such webpages and documents do not get discovered by search engines.					✓				✓
5. Limit the number of failed logins This plays a part in preventing brute force attacks. Various mechanisms can be implemented, such as: • locking the account after 'x' number of failed attempts; • requiring an increasing amount of time; before a login retry can be attempted; and • using Captcha (against automated brute force attacks).	✓	✓	✓			✓	✓	✓	
6. Implement the use of one-time passwords ("OTP") or multi-factor authentication This prevents brute force attacks and other forms of hacking. It is especially useful in securing administrative accounts or where the personal data that can be accessed after login is considered to be more sensitive.	✓	✓	✓			✓	✓	✓	

Good Practices	SDLC Phase						Tier		
	Requirements	Design	Development	Testing	Deployment	Maintenance	Presentation	Application	Data
7. Implement password complexity rules Ensure that passwords used conform to industry recommended complexity rules, e.g. each password could be having at least 8 characters in length and including at least 1 letter in caps, 1 number and 1 symbol. Also consider disallowing 'x' number of previous passwords used by the user to be reused.	✔	✔	✔			✔	✔	✔	
8. Protect passwords Protect passwords during transmission (e.g. by using encrypted transmission such as HTTPS) and during storage (e.g. by storing hashed values only). Review the method of encryption (e.g. algorithm and key length) periodically to ensure that it is recognised by the industry as relevant and secure. Protect passwords onscreen by showing only placeholder symbols such as asterisks or dots. Some applications provide users with an option to switch to show the actual password when they are certain that it is safe to do so (i.e. no one else is looking at their screens).	✔	✔	✔			✔	✔	✔	✔
9. Require regular change of passwords Consider the sensitivity of the personal data when deciding how frequently users should be made to change their passwords. Also note that requiring users to change their passwords too frequently may result in them having "password fatigue".	✔	✔	✔			✔		✔	

Good Practices	SDLC Phase						Tier		
	Requirements	Design	Development	Testing	Deployment	Maintenance	Presentation	Application	Data
10. Define user roles or groups and assign appropriate user access rights accordingly Use the "least privilege" principle to grant as little access rights as possible and assign users to the appropriate roles. As a guide, users should not be able to see information that they don't need to know. For example: • Users from the Human Resource ("**HR**") department can only view employee records and not customer records. • Within the HR department, only senior HR users can view sensitive information about employees. These examples show granular access control to personal data.	✓	✓	✓			✓		✓	
11. Log successful and failed logins Recording failed logins may help to detect or investigate hacking attempts. Some form of monitoring of logs is required to be able to detect hacking.	✓	✓	✓			✓		✓	
12. Regularly review user accounts This ensures that all user accounts are legitimate. There should be processes to update or remove user accounts, for instance, when a user has left the organisation. Test accounts should also be removed after test activities have been completed. Separately, there should also be a process to review user accounts regularly. The review should include ensuring all the rights assigned are indeed necessary.						✓			
13. Log access to sensitive data Organisations can consider logging access to personal data, especially those considered to be of higher sensitivity.	✓	✓	✓			✓	✓	✓	

TESTING OF ICT SYSTEM

Besides ensuring that the application works as expected in terms of functionality, it is important to factor in adequate resources to conduct relevant security testing and to ensure that the data protection measures operate as intended.

Good Practices	SDLC Phase						Tier		
	Requirements	Design	Development	Testing	Deployment	Maintenance	Presentation	Application	Data
1. Avoid loading production data to test environments Developers may find it tempting to load production data (often containing personal data) to test environments out of convenience. However, test environments are typically much less secure compared to production environments. Hence, such practices put personal data at risk. Organisations may consider creating synthetic data for test environments instead of using production data. For more information, refer to PDPC's *Guide to Basic Data Anonymisation Techniques.*			✔	✔		✔			✔
2. Check SQL joins Some SQL statements can be very long and consist of complex SQL joins. Errors in joining may not be obvious, yet could potentially cause data from different data subjects to be meshed together. This could result in data breaches.	✔	✔	✔			✔		✔	
3. Conduct code review Code reviews should be conducted at least for sections of source code assessed to be of high impact. If done manually, it makes sense for the review to be conducted by a relatively experienced developer.			✔	✔		✔	✔	✔	✔
4. Conduct vulnerability assessment This refers to checking if the system contains any vulnerabilities such as using unpatched components having known vulnerabilities. It is usually done using software tools.			✔	✔	✔	✔	✔	✔	

Good Practices	SDLC Phase						Tier		
	Requirements	Design	Development	Testing	Deployment	Maintenance	Presentation	Application	Data
5. Conduct penetration testing Specialised skills are required for penetration testing and organisations may engage external parties to assist if necessary. The objective is to identify how to break into the ICT system and hence identify and remedy any vulnerabilities.				✓		✓	✓	✓	✓
6. Conduct user acceptance testing ("UAT") Besides verifying system functionality, UATs can also be used to verify ease of use of the data protection measures and users' understanding of data protection policy and practices, as presented by the system.				✓	✓	✓	✓	✓	✓

ACCESS, CORRECTION AND ACCURACY OF PERSONAL DATA IN ICT SYSTEMS

ICT systems can help fulfil an organisation's obligations for Access and Correction, as well as Accuracy under the Personal Data Protection Act ("**PDPA**").
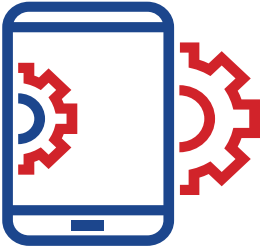
Good Practices	SDLC Phase						Tier		
	Requirements	Design	Development	Testing	Deployment	Maintenance	Presentation	Application	Data
1. Provide users with a self-management facility Where possible, allow users to manage their personal data without requiring employee assistance. This minimises the possibility of human error as well as reduces employee effort and time. This could be done through a portal, for example. Note that it is important for the portal to require users to log in before they can access their own data.	✓	✓	✓			✓	✓	✓	
2. Ensuring that user updates are done The next step is to ensure that users use the self-management facility. This can be done in various ways, such as by periodically reminding users to do so, or making sure users view their details and acknowledge that they are correct.	✓	✓	✓			✓	✓	✓	

HOUSEKEEPING OF PERSONAL DATA IN ICT SYSTEMS

Organisations usually focus on protecting their main source of personal data (e.g. their database) but may neglect to protect secondary storage locations of personal data, which are often somewhat temporary or one-time in nature. Hence, housekeeping is especially relevant to these secondary sources.

Good Practices	SDLC Phase						Tier		
	Requirements	Design	Development	Testing	Deployment	Maintenance	Presentation	Application	Data
1. Avoid letting temporary files containing personal data become permanent Such temporary files could be generated, for example, as an intermediate form for interfacing with other systems. Protect such temporary files while they exist, and remove them once they are not required. Schedule the removal such that housekeeping is performed automatically.		✓	✓		✓	✓		✓	✓
2. Be careful with data migration files These files require extra care because the personal data could be in a more vulnerable form, for example, in a CSV file instead of in the database which is protected (typically) by layers of security. There is also the danger of the data migration phase dragging on and resulting in the vulnerability existing for a prolonged period. This can result in data migration files being forgotten even after the migration is completed, leading to permanent vulnerability.		✓	✓		✓	✓			✓

USER DEVICE SECURITY

Securing the computing devices used by employees has become increasingly important because of the prevalent mobility of computing devices. Laptops and tablets are commonplace. Any of an organisation's computing devices (brought anywhere by employees) could be an entry point to the organisation's ICT system and the personal data it contains.

For more information, refer to the sections "Personal Computers and Other Computing Devices" and "Portable Computing Devices & Removable Storage Media" in PDPC's *Guide to Securing Personal Data in Electronic Medium.*

Good Practices	SDLC Phase						Tier		
	Requirements	Design	Development	Testing	Deployment	Maintenance	Presentation	Application	Data
1. Secure employees' computing devices Common good practices that should be considered include the following: • Having policies to govern device usage • Adopting mobile device management (e.g. remote wiping) • Encrypting data on device • Implementing secure erasure of data • Using of anti-malware software • Minimising storage of personal data on device • Mandating login to device • Activating screen lock upon inactivity				✔	✔	✔			

EXPORTING DATA

There is often the need to export data to a standalone file (e.g. a report in PDF format), or transfer data to another ICT system. Once data is exported, it is "offline" and no longer protected by the access control mechanism of the originating application. Hence, do protect data in its exported form.

Good Practices	SDLC Phase						Tier		
	Requirements	Design	Development	Testing	Deployment	Maintenance	Presentation	Application	Data
1. Encrypt exported data There are various encryption algorithms available. The strength of the encryption depends on the algorithm used as well as the length of the encryption key. It is important to manage and protect the encryption keys well, including keeping the encryption key secure and separate from the encrypted data. Review the method of encryption (e.g. algorithm and key length) periodically to ensure that it is recognised by the industry as relevant and secure.	✔	✔	✔			✔		✔	
2. Communicate encryption key separately If there is a need to provide an encryption key to the receiving party of the exported file, communicate the key separately. For instance, if the encrypted file is sent by email, the encryption key should be sent via another email, or even better, another communication channel.	✔	✔	✔		✔	✔		✔	
3. Apply anonymisation techniques It is sometimes sufficient to provide anonymised values instead of the original ones. Anonymisation techniques include character masking, pseudonymisation, generalisation and data aggregation. This also applies when displaying personal data onscreen. E.g. An organisation lists a partially-masked bank account number in a monthly statement, to be used for GIRO deduction. For more information, refer to PDPC's *Guide to Basic Data Anonymisation Techniques.*	✔	✔	✔			✔	✔	✔	

Good Practices	SDLC Phase						Tier		
	Requirements	Design	Development	Testing	Deployment	Maintenance	Presentation	Application	Data
4. Utilise privacy preservation technologies New technologies that focus on protecting personal data while sharing or making use of it are emerging. These include differential privacy, homomorphic encryption, secure multi-party computation, etc. However, at the time this Guide is published, only some of these technologies are starting to be available in the form of software products.	✓	✓	✓			✓	✓	✓	
5. Sending emails Organisation should perform thorough testing before using its application to send out emails that contain personal data. This is because automated sending means a huge volume of emails could be sent in an instance, likely with no way to stop the sending out or retrieve the sent emails even if one discovers that personal data has been sent to the wrong parties. When sending the same email to multiple parties, it is recommended to place the email recipients under the "Bcc" field, especially where there could be any sensitivity involved. Instead of sending personal data directly in emails, one can send emails containing a link for users to access the information after authentication.	✓	✓	✓	✓		✓		✓	
6. Monitor data export activities Consider configuring a threshold of allowable data export. Also, monitor data export activities to detect data exfiltration.					✓				✓

RETENTION OF PERSONAL DATA IN ICT SYSTEMS

With data in electronic form, it should be easier for ICT systems to help organisations detect personal data that have reached the end the retention period. To achieve this, it is crucial for the system to incorporate the required design elements from the start.

Good Practices	SDLC Phase						Tier		
	Requirements	Design	Development	Testing	Deployment	Maintenance	Presentation	Application	Data
1. Manage expired personal data properly ICT systems can help to flag out records which have reached the end of the retention period. These records should be deleted or handled according to policy (e.g. be anonymised).	✔	✔	✔			✔	✔	✔	✔

MAINTENANCE PHASE

After the ICT system has gone live and stabilised, it is typical for the technical team to be scaled down in terms of manpower and other resources. However, it is important to keep sufficient resources to provide care for the personal data. Any system enhancements done at this phase can be considered as a "mini-SDLC" for the enhancements. It is thus important to review the practices recommended for earlier phases should system enhancements be performed during the maintenance phase.

Good Practices	SDLC Phase						Tier		
	Requirements	Design	Development	Testing	Deployment	Maintenance	Presentation	Application	Data
1. Watch out for new or updated legal requirements Laws change over time. Hence, requirements and obligations relating to personal data may also change.						✔	✔	✔	✔
2. Watch out for technology changes Similarly, technology changes may require tweaks to be made in the system design or implementation. For instance, encryption standards which are regarded as secure today may eventually be considered no longer secure or a good practice.						✔	✔	✔	✔
3. Keep data inventory updated Update the personal data inventory when changes are made to the system.						✔	✔	✔	✔
4. Continue to run security tests periodically Security testing should not end when the system goes live. Even without any changes in the system, new vulnerabilities can emerge. Configuration changes in the system can also result in vulnerabilities.						✔	✔	✔	✔

ACKNOWLEDGEMENTS

We would like to express our appreciation to the following organisations for their valuable inputs in the development of this Guide:

AsiaDPO

Cyber Security Agency of Singapore (CSA)

Government Technology Agency (GovTech)

The Law Society of Singapore

SGTech

Singapore Computer Society (SCS)

The Software Alliance (BSA)

JOINTLY DEVELOPED BY