PERSONAL DATA PROTECTION COMMISSION
SINGAPORE

GUIDE FOR PRINTING PROCESSES FOR ORGANISATIONS

Published 3 May 2018

TABLE OF CONTENTS

PURPOSE OF THIS GUIDE

This Guide aims to assist organisations and print vendors to have in place adequate measures in its printing processes to protect the personal data in its possession and/or control against unintended disclosure.

While the topics listed in this Guide aim to provide recommendations for organisations and print vendors to enhance their printing processes, the topics are not exhaustive and do not address every obligation in the Personal Data Protection Act ("PDPA").

Organisations would need to take into considerations the types of personal data, corresponding sensitivity and its business model to decide on the most adequate measures to reasonably safeguard the personal data used in the printing jobs to adhere to the Protection Obligation under the PDPA.

INTRODUCTION

Printing, which encompasses mail merging and emailing, is a common and frequent activity that takes place across many organisations. For some, printing forms the core of the organisational business. More often than not, the process consists of a considerable amount of data to be printed in bulk and that may include personal data.

Why it is important to have adequate processes throughout the printing life cycle

A printing life cycle typically encompasses many layers i.e. pre-printing sorting of data, actual printing, enveloping etc.

Any layer could be susceptible to data mismanagement or negligent act, resulting in an unintended data breach incident

When an organisation outsources the printing to a print vendor, adequate contractual safeguards and process oversight are important to ensure the print vendor adheres to stipulated policies and practices

Data breaches are costly and leads to reputational loss and a decline in consumer trust.

Organisations should be aware of potential vulnerabilities in their printing life cycles, so that security arrangements can be implemented to protect the personal data in throughout the printing life cycle.

PDPA OBLIGATIONS

Organisations are required to comply with the PDPA's provisions on data protections, found in Parts III to VI of the PDPA ("**Data Protection Provisions**"), unless any exceptions under the PDPA apply.

This Guide focusses primarily on the Protection and Retention Obligations specifically in relation to the printing life cycle for:

a) In-house printing by **organisations**; and
b) **Print vendors**.

Where relevant, **organisations** may also be subject to other obligations in the PDPA i.e. Consent Obligation, Notification Obligation and other industry-specific laws that require them to protect personal data.

IN-HOUSE PRINTING BY ORGANISATIONS

PRINT VENDORS

Protection Obligation (PDPA section 24)

An organisation is required to make reasonable security arrangements to protect the personal data in its possession or control from unauthorised access or disclosure, amongst other risks.

Retention Obligation (PDPA section 25)

An organisation shall cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that (*a*) the purpose for which that personal data was collected is no longer being served by retention of the personal data; and (*b*) retention is no longer necessary for legal or business purposes.

KEY PRINCIPLES

This section describes several key principles for organisations to consider when designing controls to prevent unauthorised disclosure via their printing processes.

- ✓ **Segregation** of the roles of do-er and checker to ensure independence of the process and to make clear what each other's scope of responsibilities are.
- ✓ **Competence** of the checker i.e. Fully trained on the methods of checking.
- ✓ **Documentary trail** of the actions of do-er and checker to ensure accountability.
- ✓ **Intensity and extent** of check(s) should be proportionate to the volume and sensitivity of the personal data present in the printing process.
- ✓ **Appropriate juncture** for the check(s) i.e. performed at a suitable stage for corrective actions to be able to reverse and/or eliminate any potential error(s).
- ✓ **Well-trained** employees with clear understanding on the workflow as well as the handling of exceptions i.e. who to turn to in times of doubts and inconsistencies.
- ✓ **Contingency plans** should be well-documented and communicated in the event of a data breach event.

DATA INVENTORY MAP

A Data Inventory Map ("**DIM**") comprises a consolidation of all the data in the possession and/or control of an organisation.

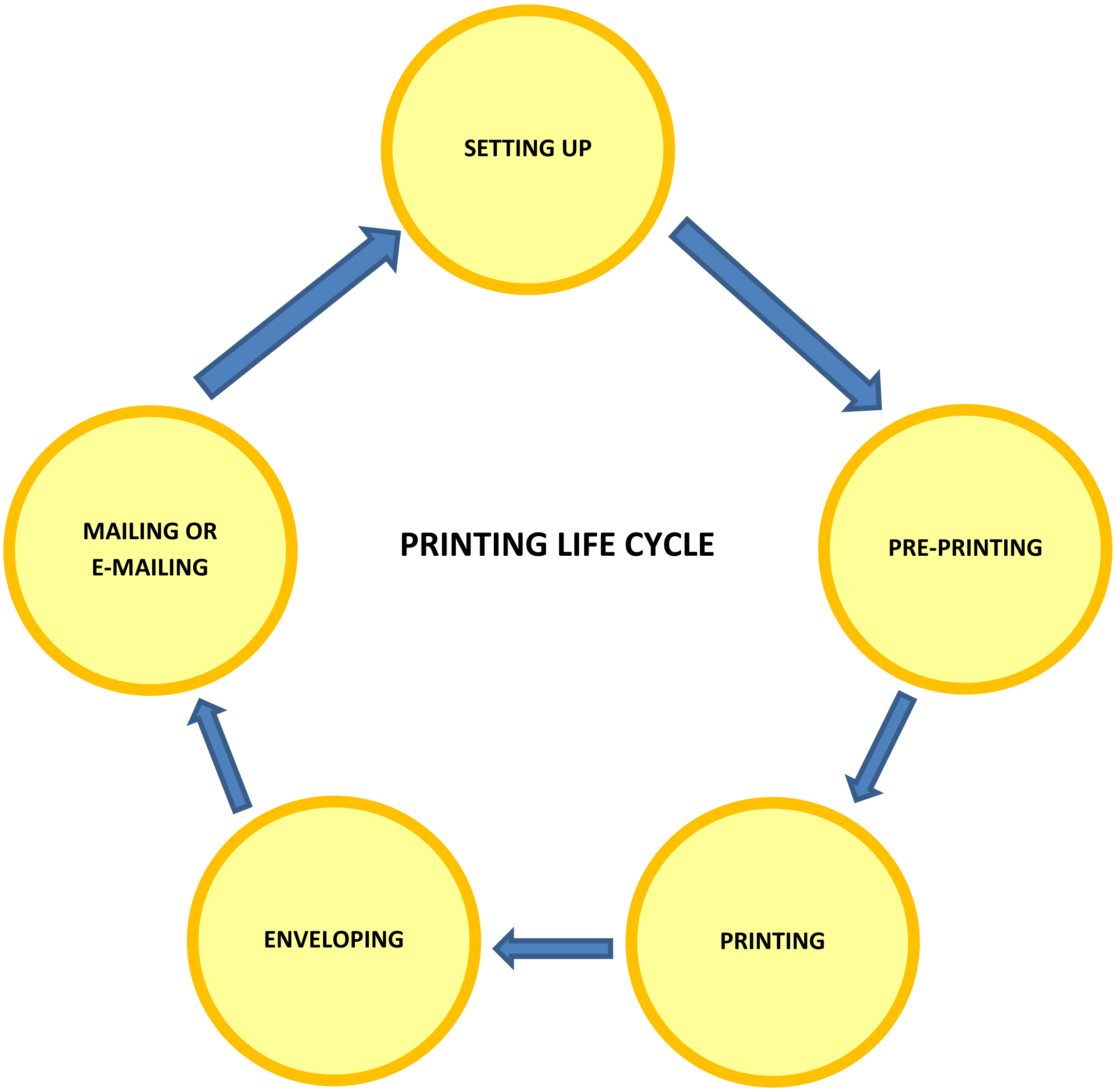
DIM helps to…

- ✓ **LIST and CONSOLIDATE** the personal data involved for each printing job.
- ✓ **IDENTIFY and CLASSIFY** the types and sensitivity of personal data for each printing job.
- ✓ **IDENTIFY** the department(s) and/or employee(s) responsible for the type of personal data for each step of the printing life cycle.
- ✓ **LIST** the contact points in event of a data breach and/or security breach.
- ✓ **ASSIST** organisations to formulate measures to protect the personal data corresponding to its risk in the event of unauthorised disclosure of personal data.

- ✓ Using a DIM will make it easier for organisations to be aware of potential flaws in each part of the printing life cycle, and to design adequate measures to correct these flaws.

THE PRINTING LIFECYCLE

The printing lifecycle of an organisation usually consists of 2 types: manual and automatic. The following section lists the broad considerations and suggested steps that organisations should be aware of while engaging in the printing lifecycle.



Setting Up

CHECK THAT SOFTWARE IS WORKING CORRECTLY

When using software to process data for printing, organisations should:

- Conduct robust acceptance tests that include all foreseeable scenarios including incorrect or incomplete inputs.
- Ensure that software is updated when new printing jobs are added, before performing the required tests.

Pre-printing

SORTING

Ensure the personal data involved i.e. names and addresses are not mismatched after sorting or mail merging, by using the correct sorting technique.

DATA ACCURACY

Check that the sorted personal data are correct, by instituting **second layer checking and/or random sampling** to reference against **source data.**

CONTACT DETAILS

Check that organisational contact details i.e. fax or address are updated should they be printed alongside the personal data

TEST RUN

Perform **test runs** and check that the intended results are returned.

Printing

SUPERVISORY CHECKS

Consider dividing the print job into batches and conduct a random sampling check to verify **accuracy of personal data.** Alternatively, random sampling check could also be performed by trained employee across the entire printing job should that be more applicable for a specific printing job.

Enveloping

LETTERS WITH ATTACHMENTS

Supervisory checks - Implement **second layer checking and/or random sampling where appropriate** to ensure that recipients match for the letter and attachment(s).

LETTERS WITH RETURN ENVELOPES

First, to ensure that return envelopes contain updated and/or correct addresses and/or contact details and secondly, to check that the accurate return envelopes are inserted to prevent return of envelopes to unintended recipients.

Mailing

MAIL ROOM

Ensure that only **authorised personnel** are permitted to enter Mailing Room to prevent instances such as theft. A documentary record could be considered for auditing purposes.

E-Mailing (via Mail Merge)

GENERATION OF EMAILS

Ensure the accuracy of the list of intended recipients and the corresponding merged fields in the email. Thereafter, conduct random sampling checks using Preview function to ensure accuracy of **personal data**.

SENDING THE EMAIL

Supervisory checks - Implement **second layer checking and/or random sampling where appropriate** to preview the email results prior to sending

OTHER CONSIDERATIONS

Aside from the main printing lifecycle, the organisations should also be mindful of the following areas of concern and its corresponding recommendations.

Data Retention

RETENTION PERIOD

Should personal data reside in the printing database after each printing job and would have no further business or legal use, to consider **specifying a period for deletion. A retention schedule will be useful in this case.**

Maintenance

INSPECTION SCHEDULE

Prepare an **inspection and/or maintenance schedule** to make sure the machinery in print life cycle is functioning according to requirements i.e. test prints.

Training and Awareness

ONGOING TRAINING FOR EMPLOYEES

Schedule employees for **refreshers and/or training** to make certain that they are up to date with the latest processes involving the printing life cycle. To enhance their understanding of the PDPA to increase vigilance in that their actions in handling personal data would comply with the PDPA.

SUPPORT AND RESOURCES

Ensure that accurate support and resources are readily on hand for employees to seek guidance on matters relating to the PDPA in the course of their work.

Disposal of Personal Data

PHYSICAL MATERIALS

Ensure that print material containing personal data that is no longer required, is disposed of securely. Please refer to PDPC's Guide to Disposal of Personal Data on Physical Medium, for good practices on secure paper disposal.

ELECTRONIC MATERIALS

Ensure that personal data that is stored electronically and no longer required is securely deleted. Please refer to Chapter 8 of the Guide to Securing Personal Data in Electronic Medium, for good practices on secure deletion.

Management of Data Breach Incidents

CONTINGENCY PLAN

Have in place a plan to manage data breach incidents and **communicate it clearly** to all employees. The plan should include procedures for the reporting and handling of incidents involving the printing lifecycle.

Please refer to PDPC's Guide to Managing Data Breaches for more information.

OUTSOURCING

Some organisations may choose to outsource the printing (e.g. via external printers) and distribution of material (e.g. via external mail and email operators) containing personal data. This section outlines some considerations for both organisations that outsource, as well as the print vendors they engage.

Key Considerations for Organisations

- ✓ The terms of the **contract** with the print vendor.
- ✓ How personal data is **transferred** to the print vendor.
- ✓ The print vendor's **processes** for checking and ensuring that mailers are sent to the correct individuals.
- ✓ Conducting **checks or audits** to ensure that the print vendor is following the correct processes.

Contractual Terms

As defined by the PDPA, a **Data Intermediary** is an organisation who processes personal data **on behalf** of another organisation. As they handle personal data in the process of printing, **print vendors are considered Data Intermediaries**.

Data Intermediaries are responsible for ensuring that they meet the **Protection** and **Retention Limitation** obligations of the PDPA. This means that they should have reasonable measures in place to **protect** the personal data entrusted to them, as well as have policies in place to ensure that personal data is **not retained** after it is no longer necessary.

When preparing the contract with an outsourced printer, organisations should consider including contractual terms that cover the following:

- PDPA obligations of the print vendor.
- The responsibilities of each party during the setup and execution of the printing process.
- The policies to be implemented by the print vendor, to ensure that PDPA obligations are met.
- Right of the organisation to review the processes of the outsourced printer, to ensure that they are following the agreed procedures.
- The specific procedures for the handling of printing jobs, especially supervisory checks to prevent the accidental disclosure of personal data.
- Procedures for the disposal of personal data, after they are no longer required.

Data Transfer

When transferring content to the print vendor for printing, organisations should be aware of the risks, and take steps to prevent accidental disclosure of personal data within the content.

Other measures to protect personal data during transfer include:

- Ensuring that emails containing personal data are sent to the correct recipient.
- Password protect the personal data before sending via email.
- Using other electronic means of transfer like Secure File Transfer Protocol (SFTP).
- Securing the portable media (e.g. encrypting the thumb drive’s content or relevant files) when making a physical transfer.
- If using unsecured portable media, to password protect the content before copying it onto the media;

ADDITIONAL RESOURCES

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

Advisory Guidelines

- Can be found on the PDPC website at https://www.pdpc.gov.sg/ag
- Chapter 17 (The Protection Obligation) of the Advisory Guidelines on Key Concepts in the PDPA
- Chapter 18 (The Retention Limitation Obligation) of the Advisory Guidelines on Key Concepts in the PDPA
- Chapter 19 (The Transfer Obligation) of the Advisory Guidelines on Key Concepts in the PDPA
- Chapter 7 (Online Activities) of the Advisory Guidelines on the Personal Data Protection Act for Selected Topics

Other Guides

- Can be found on the PDPC website at https://www.pdpc.gov.sg/og
- Guide to Securing Personal Data in Electronic Medium
- Guide to Disposal of Personal Data on Physical Medium
- Guide to Managing Data Breaches

END OF DOCUMENT

BROUGHT TO YOU BY

PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

This publication gives a general introduction to considerations for protecting personal data in the printing life cycle in organisations and their print vendors. The contents herein are not intended to be an authoritative statement of the law or a substitute for legal or other professional advice. The PDPC and its members, officers, employees and delegates shall not be responsible for any inaccuracy, error or omission in this publication or liable for any damage or loss of any kind as a result of any use of or reliance on this publication.