GUIDE TO PREVENTING ACCIDENTAL DISCLOSURE WHEN PROCESSING AND SENDING PERSONAL DATA

Published 20 January 2017

TABLE OF CONTENTS

1 INTRODUCTION

1.1 The Personal Data Protection Act [1] (PDPA) requires an organisation to make reasonable security arrangements to protect personal data in its possession or under its control in order to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. The protection of personal data also includes preventing accidental disclosure of personal data by sending such data to the wrong recipients. Organisations that process and send documents or communications containing personal data should ensure that they have policies and procedures in place to prevent the sending of the documents or communications to the wrong recipients.

1.2 For example, organisations that prepare account statements (e.g. bank or insurance statements) to be mailed to individuals should take steps to ensure that the statements or the envelopes they are placed in, or the emails they are attached in, are not sent to the wrong recipients by using incorrect postal or email addresses; or enclosing the statement of another individual.

1.3 This guide highlights good practices for organisations that process and send physical documents or electronic communications containing personal data, be it for their own purposes, or on behalf of and for the purposes of other organisations (e.g. services handling mail merging and enveloping of documents). The practices suggested in this Guide are not meant to be exhaustive and organisations should determine the most appropriate measures to adopt given their specific circumstances.

2 MEASURES TO PREVENT SENDING OF PERSONAL DATA TO WRONG RECIPIENTS

2.1 The following are some measures that organisations should consider adopting to prevent the unauthorised disclosure of personal data:

Ensure destination information is correct

- Implement automated processing of documents or communications containing personal data (e.g. merging content or populating fields from various sources). Ensure the accuracy and reliability of the automated processing implemented by checking these systems and processes regularly. Where the data is more sensitive,

[1] Section 24 of the PDPA.

consider incorporating additional checking mechanisms to cater for unexpected situations and ensure no error arises from the automated processing.

- As good practice, establish procedures to include additional checks following the processing, printing and sorting of documents to ensure that the destination information (e.g. mailing address, email address or fax number) is correct and matches that of the intended recipient(s) prior to sending.

- For sending of emails, ensure staff perform regular housekeeping of auto-complete[2] email list and double check recipients' email addresses before sending out emails or documents containing personal data and/or sensitive data.

- For sending of mass emails on a regular basis, staff should use mailing lists where possible, instead of typing out each email address manually which may be prone to inaccuracy.

Ensure personal data to be sent is correct

- Establish procedures for staff to perform additional checks to ensure the right document containing personal data, or the right personal data contained in the document, is sent.

- For sending of emails, double check that the right files (i.e. containing the correct personal data) are attached in the email. When in doubt, files should be checked to verify that it is for the intended recipient.

Ensure only the relevant personal data is disclosed to the recipients

- Establish a policy for sending compiled sets of personal data of different individuals (e.g. in spreadsheets). Consider whether it is necessary to send the entire set of personal data of all individuals, and whether the relevant personal data of specific individuals intended for the recipient can be extracted or the personal data of other individuals can be removed before sending.

- Ensure there is consent from individuals to send their personal data to recipients other than themselves.

[2] Auto-complete email list is a feature of email software which displays suggestions for names and e-mail addresses as the user starts to type them. These suggestions are possible matches from a list of commonly used names and e-mail addresses.

- Implement email procedures to ensure all emails sent externally to a group of recipients have the recipients' email addresses placed in 'bcc' fields to avoid disclosing recipients' email addresses to all other recipients of the email.

Ensure correct usage of software

- Ensure that staff are trained and familiar with the software used to process and send out documents containing personal data. For example, staff using spreadsheets should be aware of how sorting the data incorrectly may lead to errors, for example, mismatched name and address columns. Staff should also be trained to spot any mismatched data after sorting has been carried out.

- Establish clear, step by step procedures when using software to send out emails (e.g. mailing list software). This may include ensuring that the software is configured correctly and updated regularly, and that the correct email addresses are used.

2.2 Organisations may also wish to consider whether it would be appropriate to implement the following measures to minimise the risks and impact of any accidental disclosure of personal data to the wrong recipients.

Ensure sensitive personal data is secure when sending

- Documents or communications that contain sensitive personal data should be processed and sent with particular care. Organisations could establish an email policy for documents containing personal data to be secured with passwords when sending to internal as well as external recipients.

Use notices in communications

- Include a notice in all emails, faxes and letters to warn recipients against the unauthorised use, retention or disclosure of personal data, and to inform the recipients to delete and notify the organisation immediately of any personal data sent to them in error.

Provide regular staff training

- Ensure that new and existing staff receive regular training so that they are well apprised and updated on the proper procedures for processing and sending personal data. They should also be regularly reminded to perform the necessary

checks and not become complacent relying on the system alone. Similarly, staff should not just 'click through' any alerts, but diligently verify the alert information.

2.3 Appendix 1 summarises the above in a checklist of good practices for organisations that process and send personal data.

2.4 Organisations that outsource the processing, printing and distribution of material containing personal data (e.g. to printing companies) should ensure that their vendors have in place policies and procedures to protect the personal data. Organisations should review these policies and procedures periodically to ensure that they are observed and updated as necessary. Please also refer to Appendix 2 for a checklist of good practices when outsourcing the processing and sending of personal data.

2.5 The above is not an exhaustive list and organisations may have unique processes that may not be provided for above.

3 APPLICATION TO CASES

3.1 The following cases illustrate situations in which personal data can be sent to the wrong recipients, and certain practices that may be adopted by organisations to prevent accidental disclosures when sending personal data.[3]

Case Example 1: Error in sorting

Bank A has engaged Organisation B to provide the services of printing, preparing and sending out documents to Bank A's clients. Due to human error by a staff of Organisation B, a batch of documents was erroneously sorted and inserted into envelopes addressed to the wrong recipients. As a result, some of Bank A's clients received documents that included sensitive personal data of other clients.

Learning points: Organisation B could establish policies and procedures that provide for additional layers of checks to prevent human error during the sorting process. These additional checks should ensure the accurate matching of the documents with the intended recipients and the destination addresses. Organisation B could also implement regular training for staff processing the personal data to ensure that all staff are aware and updated on the operational processes. Bank A should implement clear instructions and timely updates on new requirements to Organisation B. For example, if Bank A's document templates are to be changed (e.g. layout, paper size), Organisation B should be provided

[3] The practices suggested in this Guide are not meant to be exhaustive and complying with the suggested practices alone does not mean that an organisation is in compliance with the PDPA.

with the necessary information in order to make adjustments to its operating processes to ensure the accurate matching and sending of sensitive personal data to intended recipients.

Case Example 2: Sending compiled information

At the request of certain individuals in a tour group, Travel Agency A emailed a spreadsheet containing the personal data of all individuals on the tour group to the requesting individuals, to be used as supporting documents for their travel insurance claims. The excel spreadsheet not only contained the requesting individuals' personal details (e.g. names and passport numbers), but also that of all the other individuals in the tour group not part of the insurance claims and whose consent was not obtained to disclose their personal data for this purpose.

Learning points: Travel Agency A could establish policies and procedures on the handling of customers' requests for their personal data. This should include operating procedures to ensure that staff extract only the relevant personal data to be sent separately to each requesting individual so that the individuals only receive their own personal data. Travel Agency A should also implement regular training for staff handling personal data to ensure they are aware and updated of the proper operational procedures.

Case Example 3: Disclosing email addresses of recipients

Retail Company A sent out a mass marketing email to all its members, with each of the members' email addresses in the 'To' field. Every recipient of the email is able to see the email addresses of all other recipients of the email.

Learning points: Retail Company A could establish policies and procedures that include email procedures for recipients' email addresses to be placed in the 'bcc' field of emails, or to use a group mailing list of undisclosed recipients when sending mass emails to external recipients, so as to prevent the disclosure of recipients' email addresses.

Case Example 4: Auto-completing of email addresses

Medical Clinic A intended to send an email containing its patients' health records to Laboratory B. However, due to similarities in the first few letters of Laboratory B and Client C's email addresses, the email address was wrongly auto-completed with Client C's email address, as the staff had previously added Client C's email address to a global mailing list. As a result, the email containing the patients' health records was wrongly sent to Client C.

Learning points: Medical Clinic A could establish policies and procedures that include email procedures for all staff sending emails to external recipients to perform a check of the recipients' email addresses before sending. Medical Clinic A could also implement a policy to disable the use of auto-complete feature for all external email addresses as it deals with sensitive health information. Additionally, it could also have implemented a policy for all staff to set a few minutes' delay to the sending of emails so that there is an opportunity for staff to recall the emails should they detect an error shortly after sending. Finally, Medical Clinic A should implement a policy for sensitive personal data to either be secured with passwords and/or emails to be encrypted when sending such data. Regular training for staff should also be conducted to ensure all staff are aware and updated of the latest operational procedures.

Case Example 5: Error when sorting file

Insurance Company A contracted Organisation B to send out letters to policyholders containing information on insured persons' policies. However, a staff member of Organisation B made a mistake when sorting the file containing the policyholders' names and mailing addresses. This caused the policyholders' names and mailing addresses to be mismatched. As a result, the letters were delivered to the wrong recipients.

Learning points: Organisation B could establish policies and procedures that provide for additional layers of checks to ensure that destination information (e.g. mailing address, email address or fax number) is correct and matches that of the intended recipients prior to sending, even where this process is automated by IT systems. Insurance Company A should also implement regular training for staff processing the personal data to ensure that all staff are aware and updated on the operational procedures, as well as the proper use of its IT systems and software.

3.2 The following cases illustrate how organisations have implemented practices to prevent accidental disclosure of personal data.

Case Example 6: Managing public queries

Organisation C has a call centre that receives email enquiries containing personal data in the email body or in email attachments. The scope of work requires Organisation C's call centre staff to forward the emails enquiries to colleagues in other departments within the same organisation for processing, which includes replying to these emails.

To reduce the incidence and the impact of emails containing personal data wrongly sent to the wrong recipients, Organisation C has implemented the following measures, which are enforced by configuring the email software (e.g. Microsoft Outlook):

- All emails are sent after a delay of 1 minute.
- Autocomplete email addresses feature is disabled.
- Alert email sender when there are sensitive data within the email (e.g. NRIC, credit card numbers).
- Standardised email signature that contains a notice to warn recipients against the unauthorised use, retention or disclosure of personal data, and to inform the recipients to delete and notify Organisation C immediately of any personal data sent to them in error.

Staff of Organisation C will also have to ensure that all sensitive personal data is sent as a password protected file attachment. Staff are also required to redact unnecessary personal data when sending email enquiries within Organisation C for processing purposes.

Additionally, all staff handling personal data are given regular training to ensure they are aware and updated of the proper operational procedures.

4 RELEVANT PDPA OBLIGATIONS

4.1 While there is no one size fits all solution for compliance, each organisation should consider adopting security arrangements that are reasonable and appropriate in the circumstances; for example, taking into consideration the nature of the personal data, the form in which the personal data has been collected (e.g. physical or electronic) and the possible impact to the individual concerned if an unauthorised person obtained, modified or disposed of the personal data. Accordingly, an organisation may wish to consider adopting the practices mentioned in this Guide as part of the security arrangements it implements.

4.2 Under Section 4(2), a data intermediary may be subject to fewer Data Protection Provisions where it is processing personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing. However, in such instances, a data intermediary will nevertheless be required to comply with Sections 24 (which is mentioned above) as well as Section 25, which requires organisations to cease retention of personal data where the purpose for collection of the data is no longer served by its retention, and retention is no longer necessary for legal or business purposes.

4.3 Additionally, organisations should note that they may be held liable for the actions or omissions of its data intermediary that amounts to a breach of a Data Protection Provision. The organisation should therefore ensure that its contract with its data intermediary imposes sufficient obligations on the data intermediary to ensure the organisation's own compliance with the PDPA.

5 ADDITIONAL RESOURCES

5.1 Organisations are encouraged to refer to the PDPC website for additional resources (www.pdpc.gov.sg). Relevant guides on this topic are:

i) Advisory Guidelines on Key Concepts in the PDPA (Chapter 17 on Protection Obligation)
https://www.pdpc.gov.sg/ag

ii) Guide to Securing Personal Data in the Electronic Medium
https://www.pdpc.gov.sg/og

iii) Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data
https://www.pdpc.gov.sg/og

iv) Guide to Managing Data Breaches
https://www.pdpc.gov.sg/og

END OF DOCUMENT

APPENDIX 1: CHECKLIST OF GOOD PRACTICES FOR ORGANISATIONS PROCESSING AND SENDING PERSONAL DATA

Ensure destination information is correct		
1	Implement automated processing of documents or communications containing personal data (e.g. merging content or populating fields from various sources). Ensure the accuracy and reliability of the automated processing implemented by checking these systems and processes regularly. Where the data is more sensitive, consider incorporating additional checking mechanisms to cater for unexpected situations and ensure no error arises from the automated processing.	☐
2	Establish procedures to include additional checks following the processing, printing and sorting of documents to ensure that the destination information is correct and matches that of the intended recipient(s) prior to sending.	☐
3	Perform regular housekeeping of auto-complete email list and double check recipients' email addresses before sending out emails or documents containing personal data and/or sensitive data.	☐
4	For sending of mass emails on a regular basis, use mailing lists where possible, instead of typing out each email address manually which may be prone to inaccuracy.	☐
Ensure personal data to be sent is correct		
5	Establish procedures to perform additional checks to ensure the right document containing personal data, or the right personal data contained in the document, is sent.	☐
6	When sending emails, double check that the right files (i.e. containing the correct personal data) are attached in the email.	☐
Ensure only the relevant personal data is disclosed to the recipients		
7	Establish a policy for sending compiled sets of personal data of different individuals (e.g. in spreadsheets).	☐
8	Ensure there is consent from individuals to send their personal data to recipients other than themselves.	☐
9	Ensure all emails sent externally to a group of recipients have the recipients' email addresses placed in 'bcc' fields.	☐
Ensure correct usage of software		

10	Ensure that staff are trained and familiar with the software used to process and send out documents containing personal data. Staff should also be trained to spot any mismatched data after sorting has been carried out.	☐
11	Establish clear, step by step procedures when using software to send out emails, including ensuring that the software is configured correctly and updated regularly, and that the correct email addresses are used.	☐
Minimise impact of accidental disclosure		
12	Establish an email policy for documents containing personal data to be secured with passwords when sending to internal as well as external recipients.	☐
13	Include a notice in all emails, faxes and letters to warn recipients against the unauthorised use, retention or disclosure of personal data, and to inform the recipients to delete and notify the organisation immediately of any personal data sent to them in error.	☐
14	Ensure that new and existing staff receive regular training so that they are well apprised and updated on the proper procedures for processing and sending personal data. Staff should also be regularly reminded to perform the necessary checks and not become complacent in relying solely on automated systems. Similarly, staff should not just 'click through' any alerts, but diligently verify the alert information.	☐

APPENDIX 2: CHECKLIST OF GOOD PRACTICES FOR ORGANISTIONS WHEN OUTSOURCING THE PROCESSING AND SENDING OF PERSONAL DATA

Ensure the organisation you are outsourcing the processing and sending of personal data to:		
1	Has in place appropriate data protection policies and procedures for the work that is being outsourced.	☐
2	Has breach management protocols in place, including protocols to report any data breaches to your organisation.	☐
3	Has procedures in place to log all activities including access to and extraction of the personal data.	☐
4	Uses personal data only in line with your organisation's instructions. This could be included as a clause in the contract with the organisation undertaking the outsourced work.	☐
5	Ensures that only the relevant staff involved in the outsourced work have access to the personal data. These staff should also be well trained in complying with organisation's data protection policies and procedures (e.g. control the use and disclosure of personal data by ensuring no internal or external leakage of personal data).	☐
6	Is able to cope with the required document output volume, and possesses the flexibility required to adapt to process or workflow changes.	☐
Other measures to minimise the risks and impact of accidental disclosures:		
1	Ensure that the contract with the organisation undertaking the outsourced work can be effectively enforced.	☐
2	Conduct regular data audit checks on the organisation undertaking the outsourced work during the outsourcing agreement period to ensure that the data protection policies and procedures are adhered to. This may include carrying out an audit check after all processing under the agreement has been carried out, to ensure there is no further retention of personal data.	☐
3	Consider the possibility of the outsourced work being further sub-contracted by the organisation, and if this is permitted, put in place clear parameters for sub-contracting to ensure the sub-contractor(s) similarly has in place the necessary data protection policies and procedures for the work that is being sub-contracted.	☐

BROUGHT TO YOU BY