When Careless Printing Leads to Breaches

Mistakes in the printing process have led to a number of breaches in Singapore. Hence, the PDPC has published a Guide for Printing Processes for Organisations to help companies better manage personal data exposure risks in the printing process.

The faxes came in intermittently – between one and five were received every week. But what was unusual was the fact that they were insurance renewal submissions from customers, when the recipient was a retail company.

Between November 2016 and May 2017, an estimated 25 to 125 insurance renewal submissions were sent to the wrong party, exposing the personal details of policy holders.

This case of a wrong facsimile number being printed on the renewal notices is one recent example of an oversight in printing processes that led to unintended disclosure of personal data, putting the organisation on the wrong side of the Personal Data Protection Act (PDPA).

In another case also involving an insurance company, a mistake in duplex printing resulted in policy holders receiving letters which had, on the reverse, a letter addressed to another customer.

A third case involved a printing and enveloping company that sent financial statements to the wrong individuals, resulting in its client's account holders receiving statements that contained information of other account holders. These examples highlight the risk facing industries that need to print and send out customer information on a regular basis.

Missteps Leading to PDPA Breach

A closer examination of the three cases that were investigated by the Personal Data Protection Commission (PDPC) helps shed light on the missteps that led to a breach of the PDPA.

In the first example, AIG Asia Pacific Insurance had an incorrect facsimile number on the policy renewal notices issued to its policy holders. This led to the policy holders faxing their renewal submissions to an unrelated third party instead of AIG.

The mistake led to the exposure of policy holders' personal data because the renewal notice form contained information such as the

policy holder's name, address and policy details. Some also carried personal data of the policy holder's family members.

Upon investigation, it was found that the wrong facsimile number was inserted when an old AIG number was keyed in during the development of templates for the company's new electronic policy administration system.

The mistake went undetected because the company did not have a process in place to verify the accuracy of the facsimile number uploaded to, or in use by, its system. When conducting the user acceptance testing for the new system, there was no provision to send a test fax to verify the facsimile number. This was an "alarming" oversight as the facsimile number that was keyed in had not been in use for five years, noted PDPC.

Given that personal data was involved, PDPC said it was "incumbent" on AIG to stipulate correct and updated contact details to avoid the risk of personal data being sent to an unauthorised third party.

Inadequate Checks

In the second case, insurance policy letters addressed to two different policy holders were printed on the same sheet of paper because the print room operator had mistakenly chosen to print the letters on both sides of the paper.

Upon investigation, PDPC found that NTUC Income did not have adequate checks in place to catch the mistake. The print room operator was required to conduct a visual check on a sample of printed letters – but only for the quality of print and alignment. In addition, the checks were undertaken by the same print room operator who printed the letters. And while there was some reconciliation of the number of pages printed with the number of letters sent for printing, PDPC determined that the reconciliation check would not have been an adequate measure to detect the mistake.

As a result of inadequate security measures, personal data was disclosed without authorisation.

The third case, which took place in 2015, involved Toh-Shi Printing Singapore and its client, the Central Depository (CDP). CDP provides clearing, settlement and depository facilities for customers in the Singapore securities market.

A breach had occurred due to misalignment of pages during the sorting process, which led to errors in the compilation of multi-page CDP statements – the first page of each affected account holder was compiled with the second and subsequent pages of another account holder.

Even though the issue was detected during the compilation process, Toh-Shi's staff mistakenly discarded the correct statements and despatched the erroneous statements for postage instead. Toh-Shi failed to implement adequate operational processes to ensure that the letters with personal data were sent to the correct recipients.

Guide for Printing and Emailing

To address these common denominations and other personal data exposure risks in the printing or emailing process, the PDPC published a Guide for Printing Processes for Organisations to help businesses and print vendors put in place adequate measures in their printing processes to protect personal data in their possession and ensure that there are controls against unintended disclosure.

The guide highlights areas that organisations should pay attention to during the set-up, pre-printing, printing, enveloping, mailing and emailing phases of the printing lifecycle.

For example, the case of the wrong facsimile number could have been prevented if the organisation had conducted robust acceptance tests in the set up phase of the printing cycle. The Guide recommends that these tests should cover all foreseeable scenarios including incorrect or incomplete inputs. Another safety net would be pre-printing, when the organisation should check that contact details such as the facsimile number and mailing address are updated.

In the wake of the PDPA breach, AIG had gone on to tighten measures to reduce the risks of a similar incident. It now requires its managers to verify the accuracy of contact information for corporate use. It has also included, in the user acceptance testing process for its systems, a step to confirm that documents sent using the contact details provided are received by the intended recipient.

Given that the processes for managing printing and emailing are comparable, the Printing Guide also makes similar recommendations for the management of mass emails to customers.

Remediation Measures

In the case of duplex printing, NTUC Income should have implemented more stringent checks over and beyond the visual checks for print quality and the reconciliation of electronic print counters, given the fact that the printouts contained personal data of a sensitive nature.

This would be in line with one of key principles outlined in the Guide, which points out that the intensity and extent of checks should be proportionate to the volume and sensitivity of the personal data present in the printing process.

After the breach, NTUC Income implemented several remediation measures to prevent similar incidents from recurring. For example, both the print room and mail insertion operators are now required to compare the soft copy files sent for printing with the printed letters before enveloping. The checks will help ensure that the letters are printed in the correct format (either simplex or duplex).

Besides providing guidance for personal data protection in the main printing lifecycle, other areas covered in the Guide include data retention, maintenance of print machinery, employee training and awareness, disposal of personal data that is no longer required, and the management of data breach incidents. The Guide also provides recommendations for personal data protection in scenarios such as the outsourcing of printing and distribution of material containing personal data.

The Guide for Printing Processes for Organisations may be found on the PDPC's website at www.pdpc.gov.sg/og.