NORTHWEST TERRITORIES
INFORMATION AND PRIVACY COMMISSIONER
Review Report 20-231
Citation: 2020 NTIPC 30

File: 19-188-4, 19-192-4, 19-197-4, 19-199-4, 19-204-4
May 22, 2020

BACKGROUND

Beginning on July 15th, 2019 my office received a series of privacy breach complaints from employees of the Department of Education, Culture and Employment (ECE). On July 22, 2019 I also received a breach notification from the Department outlining the circumstances of a breach involving several employees and it was obvious that all of these reports related to the same incident. I have therefore merged all of the files and will do one report for all of them.

THE BREACH

On June 4, 2019 an email was sent by an employee of the Finance and Capital Planning Division of ECE to several recipients, mainly ECE senior management. An Excel spreadsheet was attached to the email. The spreadsheet had two tabs - one tab contained a "Signature Specimen Records" document and the second contained payroll information for departmental employees from May 2018. The purpose of the email was to ask recipients to review the contents of the first tab to ensure it was up to date. The second tab should have been deleted from the spreadsheet before it was sent. This second tab included the following information:

- Name;
- Employee ID;
- Pay status of employee (active or leave of absence);
- Employee position status (regular or temporary);
- For temporary employees, their termination date;
- Employee step on the pay grid;
- Employee rate of pay; and
- Employee annual rate.

The error was not discovered until June 24th and by that time most of the recipients had already opened the spreadsheet and it could not be recalled. The department did, however, contact all of the recipients and asked them to delete the email from their systems and confirm that deletion. All recipients, but for three who were out of the office on annual leave at the time the breach was discovered, confirmed that they had deleted the email. At the time of the breach report to my office, the department indicated that it would be following up with the three remaining recipients when they returned to the office.

In investigating how this breach happened, the department learned that the second tab including May 2018 payroll information had at some point been added to the SSR master spreadsheet to allow comparison of employee position numbers and to determine if any positions needed to be added to bring the SSR document up to date. Once the breach was discovered, the second tab of the spreadsheet was immediately removed from the master spreadsheet and staff who deal with payroll information were reminded to review all spreadsheets before emailing to ensure that they contain no personal information that should not be disclosed.

All of the affected employees were advised of the breach and an apology was provided.

DISCUSSION

Section 1 of the *Access to Information and Protection of Privacy Act* sets out the purposes of the legislation, one of which is to prevent the unauthorized collection, use or disclosure of personal information by public bodies. Section 48 outlines the circumstances in which a public body can disclose personal information. While the term "disclose" is not defined in the legislation, it has been determined that the term includes providing access to personal information to employees within the GNWT where that employee has no operational need to have that information for the purpose of performing their job, even within the same department or the same division of a department. In this case, the public body has acknowledged that there was an unauthorized disclosure of the personal information of a number of its employees. There is, therefore, no need for me to analyse whether or not a breach of privacy occurred. For the record, however, I agree that the inclusion of the pay information for individual employees on the spreadsheet that was emailed to a number of ECE employees did, in fact, amount to an unauthorized disclosure of personal information.

Once privacy is breached, there is no way to undo that breach. Steps can be taken to mitigate possible damage, but the breach cannot be undone. In this case the Department took what steps it could after the fact to mitigate the damage. Once the error was discovered, all recipients of the email were contacted and asked to delete the email and they received confirmation that this had been done. They advised the affected individuals of the breach and advised them that they had the right to ask my office to review the breach. These steps reflect best practices. I note that the reporting of breaches of privacy is not currently required under the ATIPP Act, though it will shortly become so when Bill 29 (*An Act to Amend the Access to Information and Protection of Privacy Act*) comes into effect. The department's proactive reporting of the breach to both this office and to affected individuals notwithstanding the lack of a legislated duty to do so is a positive development.

I am also satisfied that the public body took the necessary steps to determine how the breach occurred so that they could address the root cause of the breach and take steps to prevent a repeat of it in the future. They determined that an employee had used a master excel spreadsheet and, without saving a copy and using that for their work, had added a second sheet for comparison purposes which was saved with the second sheet still attached. This then became the "master" copy of the spreadsheet. The sender of the email did not think to make sure there was only one page on the spreadsheet when it was sent.

I am less satisfied that the Department took sufficient steps to ensure that this kind of breach could not occur again. While the master spreadsheet was fixed by removing the offending second page, and employees were "reminded to review all spreadsheets before emailing to ensure that all payroll information is removed", there were no steps taken to make it harder to make the same mistake again. More can be done to prevent a recurrence. For example, "master" copies of spreadsheets and databases should be saved in a manner that does not allow changes to be made to them without saving the document with another name or actually removing the protective attributes before the document can be changed. This seems to be a fairly easy fix and one that would not unduly interfere with the work of the department. At the very least, this would force the person accessing and using the spreadsheet to think about what they are doing before making changes.

I am also somewhat concerned that the breach was not discovered until 20 days after the email was sent out. I have been given no information about how the breach was discovered or by whom. I assume that one of the recipients eventually noticed the second page of the spreadsheet and reported it to the sender of the email. There was no effort to determine from other recipients of the email whether they had noticed the error and failed to report it back to the sender. Either the recipients of the email did not see or open the second page of the spreadsheet or they did not recognize that the addition of the second sheet of the spreadsheet was a breach of privacy that needed to be addressed, or, recognizing it as a breach of privacy, failed to take steps to address it. This is concerning.

Nor is there any indication that the department followed up with any of the recipients to ensure that, not only did they delete the email, but that they had not used or further disclosed any of the information in the second page of the document.

CONCLUSIONS AND RECOMMENDATIONS

The Department in this case recognized that an error had been made that resulted in the unauthorized disclosure of payroll information to a number of Departmental officials and took steps to correct the error (to the extent that it could be corrected). The live issues here for me are whether those steps went far enough and whether tools were put in place to prevent a similar disclosure in the future. I suspect that this department (and most departments) have detailed spreadsheets considered “master” spreadsheets not intended to be manipulated and changed except by specific employees whose job it is to maintain the spreadsheets. I **recommend** that these spreadsheets be identified and saved in a format that does not allow the document to be changed without another step being taken as discussed above.

I further **recommend** that all employees with the Department of Education, Culture and Employment who deal in any way with personal information be required to complete basic privacy training at the commencement of their employment, with a further requirement that this training be repeated periodically, preferably annually. There are on-line resources available for such training within the Government of the Northwest Territories and these resources should be utilized so that employees can take the training at a time that suits them, rather than waiting for an in-person course to be provided. This is a department that deals with huge amounts of personal information

and all employees should be in a position not only to recognize a breach of privacy when they see it, but also to know how to address it.

Finally, I **recommend** that the Department consider establishing a privacy breach policy, much like the one currently being used by the Department of Health and Social Services and other health information custodians subject to the *Health Information Act*. Breach notification is not currently a requirement of our legislation, but when Bill 29 comes into effect in the next few months, such notification will be required. It would definitely assist the Department to have a privacy breach policy in place that will help to guide and assist employees in dealing with privacy breaches, and ensure that all appropriate steps are taken. Having this in place before the breach notification provisions come into effect will keep the department ahead of the curve.

Elaine Keenan Bengts
Information and Privacy Commissioner