



Office of the  
Saskatchewan Information  
and Privacy Commissioner

## INVESTIGATION REPORT 262-2018

### Saskatchewan Liquor and Gaming Authority

April 15, 2019

#### Summary:

On October 31, 2018, the Saskatchewan Liquor and Gaming Authority (SLGA) informed the Complainant that a privacy breach investigation involving the Complainant's personal information had been conducted. The results of the SLGA's investigation found that there was one instance where the Complainant's personal information was *potentially* breached and that other disclosures of the Complainant's personal information were found to be compliant with subsections 29(2)(1)(i) and 29(2)(1)(iii) of *The Freedom of Information and Protection of Privacy Act* (FOIP). The Complainant requested that the Commissioner investigate all the disclosures referred to in the SLGA's letter of October 2018. The Commissioner agreed in part with the SLGA that the disclosures, actually uses, of the Complainant's personal information were made in line with subsections 28(b) and 29(2)(1)(iii) of FOIP, but found that subsection 29(2)(1)(i) of FOIP did not apply. The Commissioner also disagreed with the SLGA's characterization that a *potential* privacy breach involving the Complainant's personal information occurred. In this respect, the Commissioner found that a breach had in fact occurred but the SLGA had appropriately managed the breach.

#### I BACKGROUND

- [1] The Complainant, an employee at the Saskatchewan Liquor and Gaming Authority (SLGA), received a letter on October 31, 2018 from the SLGA informing them that a privacy breach investigation involving their personal information had been conducted. The SLGA's letter to the Complainant indicated that the results of the investigation found one instance where the Complainant's personal information was potentially breached. The letter also indicated that there were other disclosures involving the Complainant's personal

information that occurred, but those disclosures were found to be compliant with subsections 29(2)(1)(i) and 29(2)(1)(iii) of *The Freedom of Information and Protection of Privacy Act* (FOIP).

[2] According to the SLGA's letter, their investigation of the potential privacy breach and the authorized disclosures involved an email containing the Complainant's personal information, which was sent by a Regional Director to seven managers and supervisors in retail stores in Saskatoon.

[3] On November 15, 2018 and November 16, 2018, the Complainant wrote to my office to request that my office investigate the disclosures of their personal information. In their correspondence to my office, the Complainant indicated that they disagreed with the sections of FOIP that the SLGA relied on to disclose their personal information without consent. The Complainant also expressed concerns regarding the actions of an SLGA manager that resulted in the potential breach of their personal information. As stated in the SLGA's letter to the Applicant, a manager printed the email containing the personal information of the Complainant and left it in an open area where other employees could access it.

[4] On November 22, 2018, my office provided notifications to both the SLGA and the Complainant of its intention to investigate the concerns raised by the Complainant.

## **II DISCUSSION OF THE ISSUES**

### **1. Does my office have jurisdiction?**

[5] The SLGA is a government institution pursuant to subsection 2(1)(d)(ii) of FOIP. Therefore, I have jurisdiction to conduct this investigation.

### **2. Did any privacy breaches involving the Complainant's personal information occur?**

[6] In circumstances where my office is investigating an alleged privacy breach, the focus of my office's investigation is on determining whether personal information was involved and if so, whether the personal information was collected, used and disclosed in accordance with FOIP and *The Freedom of Information and Protection of Privacy Regulations* (FOIP Regulations), as well as the institution's own internal policies and procedures. My office would also assesses whether the institution took the alleged privacy breach seriously and appropriately addressed it in line with my office's *Privacy Breach Guidelines for Government Institutions and Local Authorities*, available on my office's website.

[7] In determining whether personal information is involved, I refer to subsection 24(1) of FOIP, which contains a non-exhaustive list of information that constitutes personal information:

**24(1)** Subject to subsections (1.1) and (2), "personal information" means personal information about an identifiable individual that is recorded in any form, and includes:

...

(b) information that relates to the education or the criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;

...

(h) the views or opinions of another individual with respect to the individual;

...

(k) the name of the individual where:

(i) it appears with other personal information that relates to the individual; or

(ii) the disclosure of the name itself would reveal personal information about the individual.

[8] According to the SLGA's submission to my office, and the letter to the Complainant, on October 4, 2018, a Regional Director sent an email to all SLGA Saskatoon retail store

managers to confirm that the Complainant had been disciplined. The email, which consisted of a short paragraph, confirmed that:

- the Complainant was subject to discipline – which qualifies as personal information as per subsection 24(1)(b), employment history;
- the Regional Director believed the Complainant would repeat the offence for which they were disciplined – which qualifies as personal information as per subsection 24(1)(h); and
- the email provided the full name of the Complainant in the subject line along with the other information noted in the above bullet points – which qualifies as personal information as per subsection 24(1)(k).

[9] For clarity, “employment history” referred to in the first bullet of paragraph [8] means the type of information normally found in a personnel file such as performance reviews, evaluations and disciplinary actions taken, among other information. This definition is found in my office’s online Dictionary, available at <https://oipc.sk.ca/resources/dictionary/>, and previous reports issued by my office.

[10] As some of the contents of the October 4, 2018 email contains information that qualifies as personal information of the Complainant as defined in FOIP, I find that the Complainant’s personal information is involved in these matters. I will now proceed with determining whether any privacy breaches involving the Complainant’s personal information occurred.

[11] I will first address the disclosures that the SLGA alleged were made consistent with subsections 29(2)(1)(i) and 29(2)(1)(iii) of FOIP. These disclosures occurred when managing the conduct of the Complainant.

[12] Generally, employees of an organization are expected to perform their job duties and conduct themselves in a manner that does not harm the best interests of the employer. Employers, often managers and supervisors, monitor the performance and conduct of employees to ensure employees are meeting expectations. Because the interests of an employer can vary from one organization to the next, so too can the processes involved

with monitoring employee performance and conduct. However, employers are required to establish performance management programs in accordance with employment-related statutes, standards, principles and best practices. Where an employer is subject to privacy legislation in the province, the employer must also ensure that each step of performance management and discipline comply with the applicable privacy legislation.

[13] During this investigation, the SLGA informed my office that the Complainant and the union have appealed the disciplinary actions taken against the Complainant, described in the email of October 4, 2018. That process does not have an impact on this investigation given that the Complainant has only raised concerns regarding the disclosure of their personal information without consent to managers and supervisors via the October email. The Complainant has also requested an investigation of the potential breach of their personal information that occurred when the October email was printed and left in an open area by an SLGA manager. This investigation does not involve the privacy practices related to the collection and use of the Complainant's personal information leading up to the disciplinary and follow up actions described in the October email.

[14] According to the SLGA's submission to my office, six of the seven retail store managers, who received the October email, verbally disclosed the contents of the email to other assistant managers at their respective stores. Two of those six retail store managers also verbally disclosed the contents of the email with full time staff who occasionally act in a formal supervisory role. Only one of the seven retail store managers did not disclose the information to any other individuals in their store.

[15] The SLGA's investigation report states that all the disclosures to retail store managers, assistant managers and full time staff that occasionally supervise others was consistent with subsections 29(2)(1)(i) and 29(2)(1)(iii) of FOIP, which provides:

**29(2)** Subject to any other Act or regulation, personal information in the possession or under the control of a government institution may be disclosed:

...

(1) for the purpose of:

- (i) management;
- (ii) audit; or
- (iii) administration of personnel;

of the Government of Saskatchewan or one or more government institutions;

[16] According to the SLGA investigation report, the Complainant can work in any SLGA store in Saskatoon and so any store manager, assistant manager, or full time employee with occasional supervisory duties may have management-related responsibilities over the Complainant. The SLGA investigation report states that the Complainant's conduct which led to the October 4, 2018 email being sent:

...was significant and troubling to SLGA senior management and posed significant reputational risk to the organization. Disclosing information to management personnel that there had been past issues with [the Complainant's] employment-related conduct and subsequent discipline was directly related to SLGA's management and administration of [the Complainant].

[17] A disclosure of personal information in accordance with subsection 29(2)(1) of FOIP can occur without the consent of the individual to whom the personal information pertains. FOIP does not define the terms "management" or "administration of personnel" referred to in subsection 29(2)(1) of FOIP. However, my office has defined "administration of personnel" to refer to activities related to staffing, performance review and training and development, among other things. This definition is found in previous reports issued by my office, Investigation Reports 266-2017 and 034-2018.

[18] The term "management", as defined in the *Oxford English Dictionary*, is a word that can include both the process of dealing with or controlling things or people. When matters relate to the process of dealing with or controlling people, previous reports issued by my office, Investigation Reports 266-2017 and 034-2018, indicate that "management of personnel" refers to all aspects of the management of human resources of a public body that relate to the duties and responsibilities of employees.

[19] With those definitions in mind, I find that the purpose of sharing the Complainant's personal information found in the October 4, 2018 email was for the administration of personnel as per subsection 29(2)(1)(iii) FOIP, and not for management as per subsection 29(2)(1)(i) of FOIP. Therefore, since subsection 29(2)(1)(i) of FOIP does not apply in this case, I will not discuss whether the disclosures of the Complainant's personal information were appropriate with that subsection.

[20] I must note however that since the personal information was not shared with external parties outside of the SLGA, the data transaction is a "use" and not a disclosure. Nonetheless, SLGA may still potentially rely on the same disclosure provisions in conjunction with subsection 28(b) of FOIP as follows:

28 No government institution shall use personal information under its control without the consent, given in the prescribed manner, of the individual to whom the information relates, except:

...

(b) for a purpose for which the information may be disclosed to the government institution pursuant to subsection 29(2).

[21] According to the SLGA's submission, the Complainant is a "pool employee" in Saskatoon, which is a type of SLGA employee that can work in any SLGA store in Saskatoon. The SLGA has organized its personnel within retail stores such that any retail store manager, assistant manager, or full time employee with occasional supervisory duties can observe, identify, document and act on concerns related to an employee's performance in their respective stores.

[22] As the Complainant is not assigned to one specific store in Saskatoon, the Complainant does not have one manager or supervisor assigned to them who monitors their performance and conduct, as might be the case with non-pool employees. Because of this, it is reasonable to expect that the Complainant's personal information, as it relates to the management of their performance and conduct at work, may be disclosed without their consent to retail store managers, assistant managers, or full time employees with occasional supervisory duties at any of the Saskatoon stores where the Complainant can work. Where uses of this nature may occur, the need-to-know and data minimization rules should be followed.

- [23] As noted in paragraph [8] of this report, the October 4, 2018 email sent by an SLGA Regional Director to seven retail store managers identified the Complainant by their full name. The email stated that the Complainant was recently reprimanded for their conduct related to several incidents but the email did not go into detail about those incidents or the specific disciplinary actions taken against the Complainant. The email indicates that one incident resulted in a formal complaint to head office, but the email does not elaborate on what that incident or complaint was about. The email states that the Regional Director expects the Complainant's conduct for which they were disciplined to continue, based on their own assessment of the Complainant's behavior, and the comments in this respect are limited and specific.
- [24] Given the purpose of the October email and its contents, which followed the need-to-know and data minimization rules, I find that sharing the Complainant's personal information to retail store managers and supervisors was consistent with subsection 29(2)(1)(iii) of FOIP. Furthermore, I find that the subsequent sharing by the seven retail store managers to other managers and supervisors that would have had a role in overseeing the Complainant's performance or conduct at their respective stores, were also consistent with subsections 28(b) and 29(2)(1)(iii) of FOIP. Consequently, I find that these disclosures did not result in the SLGA breaching the Complainant's personal information.
- [25] According to the SLGA's submission to my office, a couple of days after the email was sent to the seven retail store managers in Saskatoon, SLGA senior officials communicated with the seven managers to confirm that:
- information from the email was not shared with staff who would not be responsible for managing the Complainant's performance; and
  - all supervisory staff at the seven stores were aware and understood that the contents of the email are not to be shared with non-supervisory store employees.
- [26] The follow up communication with the seven retail store managers served to reinforce the expectations of the SLGA regarding the handling of the email containing the



Complainant's personal information. This was a good follow up action on the part of the institution.

[27] In their correspondence to my office, the Complainant alleged that the contents of the email at one particular store had been read out loud by a store manager to all the staff at the store, including non-supervisory staff. SLGA's submission to my office states that when managers at the store were asked about this as part of the breach investigation, the managers stated that the contents of the email was not read out loud as alleged. However, managers confirmed that the contents were shared verbally with six other individuals at that store including with an assistant store manager and five full-time staff who periodically work in a supervisory role.

[28] Substantiating that an inappropriate verbal sharing of personal information occurred is challenging without specific proof or corroboration from individuals privy to the verbal disclosures. In this case, I have no reason to believe that the SLGA managers at the store where the Complainant alleges inappropriate verbal disclosures occurred, were not forthcoming with the SLGA's privacy officer when the SLGA conducted its internal privacy breach investigation. The Complainant has not provided any information or documentation to support their allegation of inappropriate verbal disclosures; therefore, I find that it is unlikely that the contents of the email containing the Complainant's personal information were read out loud as alleged.

[29] Notwithstanding my findings that the sharing of the October email did not result in privacy breaches, I find the vague instructions provided in the email to managers and supervisors to be problematic from a privacy perspective. The October email sent by the SLGA Regional Director advised recipients to:

...keep an eye on [the Complainant] and report any issues to [Manager] so that discipline can be escalated...if you have any questions please contact [Manager]. [Manager] knows the details.

[30] Such vague instructions do not specify what type of monitoring would be appropriate under the circumstances, nor how additional concerns are to be documented and reported by those

receiving the email. Without such information, there is a risk managers and supervisors may inadvertently engage in inappropriate privacy practices, or take actions that could violate *Part IV Protection of Privacy* of FOIP.

[31] The SLGA has an internal policy, Corrective Discipline (effective July 7, 2017), that outlines how discipline may be escalated in response to an instance or recurrence of culpable misconduct. This policy applies to all SLGA employees, even those entitled to union representation and where discipline is subject to the provisions of a collective agreement. It is unclear why the October email concerning the Complainant would not have provided clearer instructions in line with the SLGA's internal Corrective Discipline policy. The SLGA also has an internal Privacy Policy that outlines the general privacy practices of the institution, in line with the requirements of FOIP.

[32] To ensure that actions taken by managers or supervisors are in line with internal policies, I recommend that future communications regarding employee performance management or discipline either refer to the appropriate SLGA policies that should be followed, or provide clearer instructions about what activities should be undertaken while respecting *Part IV Protection of Privacy* of FOIP.

[33] I will now discuss the alleged privacy breach that occurred when an SLGA manager at a Saskatoon retail store printed the October email and left it in an open area where other employees of that store could access it. The SLGA's submission to my office, and their October 2018 letter to the Complainant, states that this was a *potential* breach. The SLGA noted that the open area is not accessible to SLGA customers or the general public. I disagree with the SLGA's characterization that a *potential* breach occurred and find that a privacy breach did in fact occur when the October email was left in an open area. My office considers a privacy breach to occur when there is an unauthorized disclosure of personal information, such as allowing individuals without a need-to-know to access or view personal information without a valid reason or purpose. If the October email was left in an open area where unauthorized employees could have read its contents, a privacy breach occurred regardless of whether anyone actually viewed or otherwise accessed the email.

[34] That said, in response to what the SLGA believed to be a *potential* privacy breach, the SLGA:

- Contained the privacy breach by ensuring no other printed copies of the October email were made;
- A subsequent communication was sent to staff at the Saskatoon store where the email was printed and left out in the open area. Staff were asked to identify if they were aware of the contents of the email and advised not to further disclose the information to anyone else;
- Disciplined the manager who caused the privacy breach;
- Held coaching sessions with the store manager who caused the breach to ensure the manager is aware of their responsibilities related to managing personal information as required by FOIP;
- Informed the Complainant of what happened via letter dated October 31, 2018 and apologized for the breach; and
- Conducted a privacy breach investigation and documented all actions related to their investigation in an investigation report.

[35] I find that the SLGA took the privacy breach related to the October 2018 email being left out in an open area seriously and appropriately addressed it in line with my office's *Privacy Breach Guidelines for Government Institutions and Local Authorities*, available on my office's website.

#### **IV FINDINGS**

[36] I find that the SLGA is a government institution pursuant to subsection 2(1)(d)(iii) of FOIP therefore, I have jurisdiction to conduct this investigation.

[37] I find that the contents of the October 4, 2018 email contains information that qualifies as personal information of the Complainant as defined in FOIP, therefore I find that the Complainant's personal information is involved in these matters.

- [38] I find that the purpose of using the Complainant's personal information found in the October 2018 email was for the administration of personnel as per subsections 28(b) and 29(2)(1)(iii) of FOIP, and not for management as per subsection 29(2)(1)(i) of FOIP. Therefore, I find that subsection 29(2)(1)(i) of FOIP does not apply.
- [39] Given the purpose of the October email and its contents, I find that the use of the Complainant's personal information to retail store managers and supervisors was consistent with subsection 29(2)(1)(iii) of FOIP.
- [40] I find that the subsequent sharing by the seven retail store managers to other managers and supervisors that would have had a role in overseeing the Complainant's performance and conduct at their respective stores, were also consistent with subsections 28(b) and 29(2)(1)(iii) of FOIP.
- [41] I find that the sharing of the October email did not result in the SLGA breaching the Complainant's personal information.
- [42] I find that it is unlikely that the contents of the email containing the Complainant's personal information were read out loud at one store as alleged.
- [43] Notwithstanding my findings that the sharing of the October email did not result in privacy breaches, I find the vague instructions provided in the email to managers and supervisors to be problematic from a privacy perspective.
- [44] I disagree with the SLGA's characterization that a *potential* breach occurred and find that a privacy breach did in fact occur when the October email was left in an open area.
- [45] I find that the SLGA took the privacy breach related to the October email being left out in an open area seriously, and appropriately addressed it in line with my office's *Privacy Breach Guidelines for Government Institutions and Local Authorities*.

## V RECOMMENDATION

[46] To ensure that actions taken by managers or supervisors are in line with internal policies, I recommend that future communications regarding employee performance management or discipline either refer to the appropriate SLGA policies that should be followed, or provide clearer instructions about what activities should be undertaken while respecting *Part IV Protection of Privacy* of FOIP.

Dated at Regina, in the Province of Saskatchewan, this 15<sup>th</sup> day of April, 2019.

Ronald J. Kruzeniski, Q.C.  
Saskatchewan Information and Privacy  
Commissioner