Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 238-2018

Saskatchewan Gaming Corporation

February 28, 2019

Summary: On October 22, 2018, the Complainant submitted a privacy breach complaint to the Saskatchewan Gaming Corporation (SaskGaming), alleging that their manager had inappropriately accessed their immigration documents in the summer of 2017. The Complainant also alleged that they had previously raised these concerns in 2017 but they had gone unaddressed. SaskGaming responded to the Complainant indicating that there was no violation of privacy but did not comment on why the Complainant's concerns were not addressed in 2017. On October 23, 2018, dissatisfied with the response from SaskGaming the Complainant requested that my office investigate the matter. The Commissioner found that his office could not fully investigate the matter because neither party could provide specific details to determine whether a privacy breach occurred as alleged. However, the Commissioner found that the Complainant had in fact raised their privacy concerns in 2017 but that SaskGaming did not appropriately address them at that time. The Commissioner made recommendations regarding the need to have appropriate policies and procedures in place to manage privacy breaches and personal information.

I BACKGROUND

[1] On October 22, 2018, the Complainant, a employee of the Saskatchewan Gaming Corporation (SaskGaming), wrote to SaskGaming alleging that their manager at SaskGaming had inappropriately accessed their immigration documents from the payroll department in 2017. The Complainant's also alleged that they had previously raised this concern with SaskGaming's human resource department but never received a response. On the latter point, the Complainant asked SaskGaming for clarification as to why SaskGaming never responded to their original concerns.

[2] On October 23, 2018, SaskGaming responded to the Complainant, indicating that:

> The sharing of human resource personnel information with a manager who has employee oversight…is well within the confines of SaskGaming policy and *The Freedom of Information and Protection of Privacy Act*. As such, there was no violation of your personal privacy as per Section 28(a)(b) of the Act.

[3] The response from SaskGaming did not provide clarification as to why SaskGaming did not respond to the Complainant's original concerns.

[4] On October 23, 2018, the Complainant, dissatisfied with the response from SaskGaming requested that my office investigate the matter. On October 25, 2018, my office provided notifications to both SaskGaming and the Complainant of its intention to investigate. In my office's notification to SaskGaming, my office requested:

- details of which section of *The Freedom of Information and Protection of Privacy Act* (FOIP) SaskGaming relied on for the use of the information in question;
- details regarding how SaskGaming took into consideration the 'data minimization' and the 'need-to-know' principles when the information in question was used;
- internal investigation report; and
- copies of any relevant policies or procedures related to the matter.

II DISCUSSION OF THE ISSUES

1. Does my office have jurisdiction?

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

2. Did a privacy breach occur? If so, did SaskGaming appropriately manage the privacy breach?

[6] At the time the alleged privacy breach occurred, which was sometime in the summer of 2017 according to the Complainant, the Complainant was authorized to work at SaskGaming in accordance with a work permit. A work permit is an immigration document issued by the federal government under Canada's immigration programs, to temporary workers who are not Canadian citizens or permanent residents of Canada so that they can legally work in Canada. An individual who receives a work permit must often comply with certain conditions, such as the type of work they can do, the employer they can work for, where they can work, etc. Individuals with work permits must provide documentation to the federal government and employers to demonstrate they continue to meet the conditions of their work permit and can continue to work in Canada.

[7] Individuals who receive work permits are also provided with a Social Insurance Number (SIN) beginning with the number "9" to identify them as temporary workers who are neither Canadian citizens nor permanent residents. An individual with this type of SIN must ensure the expiry date of the SIN always corresponds to the expiry date on their immigration document authorizing them to work in Canada.

[8] In accordance with the federal government's SIN program, employers who hire individuals with a SIN beginning with a number "9" can ask to see the employee's existing immigration document to verify that it has not expired and must ensure the employee follows the conditions and time limits of their work permit.

[9] In their original response to the Complainant, SaskGaming had advised the Complainant that the sharing of human resource personnel information with a manager who has employee oversight was within the confines of the SaskGaming policy. On October 29, 2018, my office requested a copy of the SaskGaming policy that authorized this sharing of information. SaskGaming confirmed that no such policy exists but that an internal process is in place to manage employees who have work permits. As the process is not documented in any policy or procedure, SaskGaming described the process to my office in various emails, which I will summarize as follows:

a. Since 2014, as part of the year-end tasks, the Human Resources department runs a report to validate SINs starting with the number "9". This allows them to identify SINs that may soon expire and to notify employees.

b. In addition to the year-end tasks, an employee in the payroll department and another in the Human Resource department use Microsoft Outlook to set reminders for themselves of when an employee's SIN will expire. These two employees receive the new hire packages, are the first to be in contact with employees who have a SIN starting with the number "9" and also ensure that these employees have a valid work permit. As such, these two employees know from the outset when SINs will expire.

c. The Outlook reminders allow these two employees to notify the Compensation, Benefits and Staffing manager who then reviews the information. The Outlook reminders do not exist on a shared calendar and no one other than the two employees can view these reminders.

d. If the Compensation, Benefits and Staffing manager confirms a SIN will soon expire, the manager verbally notifies the employee, which is usually done via a telephone call, and advises the employee to provide updated information.

e. Regardless of whether SaskGaming identifies SINs that will soon expire via the year-end tasks or via the Outlook reminders, the employee's manager may also be notified that an employee's SIN will soon expire. This occurs only if the expiry of the SIN will have some effect to the upcoming pay period because that employee will no longer be employed at SaskGaming.

[10] In addition to describing the above process for identifying expired, or soon to be expired, SINs, SaskGaming provided my office with a copy of its "207 Freedom of Information and Protection of Privacy policy". According to this policy, the policy is meant to outline:

> SaskGaming's position on the collection, use, disclosure and overall protection of personal information, as well as direction on responding to public inquiries about gaining access to SaskGaming records under the provisions of *The Freedom of Information and Protection of Privacy Act*, 2015 (FOIPP).

[11] This SaskGaming policy provides general definitions related to the protection of personal information and provides the general position of SaskGaming as it relates to the generally accepted ten privacy principles. The policy does not outline how personal information of employees that have work permits is collected, used and shared within the institution, in accordance with FOIP. The policy also contains a general description of the internal privacy breach management process.

[12] On October 26, 2018, SaskGaming's submission to my office stated that no breach of privacy had occurred involving the Complainant's immigration documents while they were employed at SaskGaming. According to the submission, internal consultations were undertaken with the Complainant's manager who indicated that they never accessed the Complainant's immigration documents and had asked the Complainant to send their immigration documents directly to the Human Resource department. The statements made by the Complainant's manager were supported with copies of emails from the Vice-president of Risk and Compliance, as well as the Manager of Compensation, Benefits and Staffing which stated that to their knowledge, the Complainant's manager did not access the Complainant's immigration documents.

[13] Later, SaskGaming confirmed that it was through the year-end task that the Human Resources department determined that the Complainant was ineligible to work and this information was provided to the Complainant's manager so that they could follow up with the Complainant. SaskGaming stated that the Complainant's manager was not provided with copies of the Complainant's immigration documents.

[14] When the Complainant was still employed at SaskGaming, and around the time the alleged privacy breach occurred, several meetings took place to discuss the Complainant's work permit. These meetings involved the Complainant, the Complainant's manager and employees from the Human Resources department. My office made inquiries with SaskGaming as to whether it was possible that the Complainant's manager may have seen, read or otherwise accessed the Complainant's immigration documents at these meetings, or in advance of these meetings. My office clarified to SaskGaming that even though they had confirmed that the Complainant's manager did not receive copies of the documents, access extends beyond just receiving copies of records.

[15] SaskGaming confirmed on December 14, 2018, that after further discussion with the Complainant's manager, the manager stated that they "…may have seen a document related to this issue when discussing next steps regarding [the Complainant] with [a Human Resources employee]…". The Complainant's manager also stated that they have no idea

what the document was, nor recalls reading it, but recalls never requesting to see it even though it was shared with them. The Complainant's manager further stated that they spoke to the Human Resources employee who shared the document with them, but that employee was also unable to recall what the document was.

[16] 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 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.

[17] The parties involved in this case are unable to provide my office with specific information about the alleged 2017 privacy breach. The Complainant's manager recalls one incident, as described above, where they potentially saw a document involving the Complainant's work permit, but neither they, nor the employee who shared the document with them, can recall what the document was. It is possible that the Complainant's manager would have been authorized to receive and view that document for the purposes of managing employees with work permits. However, because my office cannot review the document, nor obtain details about what information was on that document, my office is unable to make this determination and assess whether a privacy breach occurred in that instance.

[18] The Complainant, on the other hand, advised my office that they do not have any emails or other records from when they were employed at SaskGaming to further support their allegations that their manager inappropriately accessed their immigration documents from the payroll department in the summer of 2017. As such, without more specific information, I find that my office is unable to fully examine the facts, investigate this alleged privacy breach and determine whether a privacy breach occurred.

[19] The Complainant's October 22, 2018 email to SaskGaming and their correspondence to my office of October 28, 2018 stated that they had previously raised their privacy breach concerns in 2017. The Complainant provided my office with proof that they had raised this issue during a meeting on September 12, 2017, which was attended by a union representative, their manager and an employee from the Human Resources department. SaskGaming provided my office with a copy of their meeting minutes related to this 2017 meeting. Their meeting minutes do not indicate that the Complainant raised concerns about a possible privacy breach involving their manager. It is unclear why SaskGaming did not record this information, nor proceed with conducting an investigation in line with its own policy related to the management of privacy breaches. In this regard, I find that SaskGaming did not take the Complainant's allegations seriously in 2017 and therefore did not appropriately address them at that time.

[20] My office expects institutions subject to FOIP to respond to privacy concerns submitted to them by individuals within approximately thirty days. The thirty-day deadline, while not specified in FOIP, provides institutions a reasonable amount of time to conduct an internal investigation into an alleged privacy breach and respond to the individual making the allegation. If SaskGaming had appropriately documented the concerns of the Complainant and investigated the allegation in 2017, they would have been able to provide my office with details of their investigation and perhaps the outcome of my investigation today would have been different.

[21] This case highlights the importance of having appropriate privacy breach management processes that defines what a privacy breach is, requires that privacy concerns be investigated within 30 days, outlines the steps involved in investigating alleged or actual privacy breaches and requires that each step of the investigation process be documented in an investigation report. The section on privacy breaches in SaskGaming's "207 Freedom of Information and Protection of Privacy policy" does not currently include these elements. I recommend that SaskGaming review and revise its "207 Freedom of Information and Protection of Privacy policy" so that it is in line with the elements outlined in my office's Privacy Breach Guidelines.

[22] This case also highlights the need for institutions to have proper written policies and procedures related to the management and protection of personal information in the administration or carrying out of programs or activities of the institution, as per the duty to protect obligations imposed by subsection 24.1 of FOIP, which provides:

> **Duty of government institution to protect**
> **24.1** Subject to the regulations, a government institution shall establish policies and procedures to maintain administrative, technical and physical safeguards that:
>
> (a) protect the integrity, accuracy and confidentiality of the personal information in its possession or under its control;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the personal information in its possession or under its control;
>
> (ii) loss of the personal information in its possession or under its control;
> Or
>
> (iii) unauthorized access to or use, disclosure or modification of the personal information in its possession or under its control; and
>
> (c) otherwise ensure compliance with this Act by its employees.

[23] As it stands, SaskGaming's "207 Freedom of Information and Protection of Privacy policy" serves more as an overarching privacy policy related to the overall protection of personal information but does not provide specific information to SaskGaming employees that have a role in overseeing or managing other employees with work permits. The processes described in the preceding paragraphs related to how expired, or soon to be expired, SINs are verified for individuals with work permits involves many employees, administrative processes and tools. It is unclear how SaskGaming expects employees, including those who have work permits, to know and understand what personal information may be collected, used, shared or retained without more specific written policies and procedures.

[24] During this investigation, SaskGaming also confirmed that the Complainant had a study permit while employed at SaskGaming in October 2017 and that managing an employee

with a study permit requires that the same processes as those described in paragraph [9] of this report be followed. As such, there are no specific policies and procedures related to the collection, use, disclosure or retention of personal information related to study permits.

[25] I recommend that SaskGaming implement a specific policy and written procedures for how the institution will collect, use, disclose and retain personal information of individuals that have, or require, work permits or study permits as per subsection 24.1 of FOIP. I also recommend that SaskGaming make the policies and procedures discussed in this report publicly available on its website in accordance with subsection 65(1)(a) of FOIP.

IV FINDINGS

[26] I find that my office is unable to fully examine the facts, investigate this alleged privacy breach and determine whether a privacy breach occurred.

[27] I find that SaskGaming did not take the Complainant's allegations seriously in 2017 and therefore did not appropriately address them at that time.

V RECOMMENDATIONS

[28] I recommend that SaskGaming review and revise its "207 Freedom of Information and Protection of Privacy policy" so that it is in line with the elements outlined in my office's *Privacy Breach Guidelines for Government Institutions and Local Authorities*.

[29] I recommend that SaskGaming implement a specific policy and written procedures for how the institution will collect, use, disclose and retain personal information of individuals that have, or require, work permits and study permits as per subsection 24.1 of FOIP.

[30] I recommend that SaskGaming make the policies and procedures discussed in this report publicly available on its website in accordance with subsection 65(1)(a) of FOIP.

Dated at Regina, in the Province of Saskatchewan, this 28th day of February, 2019.

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