Office of the
Saskatchewan Information
and Privacy Commissioner

September 28, 2023

Employment Standards Review
Corporate Services Division
Ministry of Labour Relations and Workplace Safety
300-1870 Albert Street
REGINA, SK S4P 4W1 Email: legislation.labour@gov.sk.ca

Dear Sir or Madam:

Re: The Saskatchewan Employment Act and Associated Regulations

I am pleased that the Ministry is doing a review of *The Labour Standards Act*. Please find attached my submission which focuses on privacy issues of employees of businesses and nonprofit organizations operating in Saskatchewan. The submission is based on the principle that all employees in the province should have the same protection of their personal information under provincial or federal law.

If you have any questions, please do not hesitate to give me a call at (306) 537-4287.

Yours truly,

[redacted]

Ronald J. Kruzeniski, Q.C.
Saskatchewan Information and Privacy Commissioner
rkruzeniski@oipc.sk.ca

cc Drew Wilby, Deputy Ministry of Labour, drew.wilby2@gov.sk.ca

Office of the
Saskatchewan Information
and Privacy Commissioner

Submission of the Saskatchewan Information and Privacy Commissioner To the Employment Standards Review September 28, 2023

Introduction

I am pleased that the Government of Saskatchewan has embarked upon a consultation to modernize *The Saskatchewan Employment Act* (SEA). Although the SEA can involve many issues, I will restrict my comments and suggestions to access and privacy issues that affect employees.

Current Legislation

The Freedom of Information and Protection of Privacy Act (FOIP) was passed in 1992 and has been amended from time to time. It deals with government institutions which includes ministries, Crown corporations, agencies and other organizations prescribed in the regulations. It has privacy provisions set out in Part IV, which applies to all aspects of the government institutions information practices including that of its employees.

The Local Authority Freedom of Information and Protection of Privacy Act (LA FOIP) was passed in 1993 and applies to local authorities that include cities, towns, municipalities, universities and school boards. It also has privacy provisions set out in Part IV, which applies to those involved with the local authority including employees of local authorities.

In each Act, the privacy provisions deal with the collection, use, disclosure and protection of personal information of residents and employees.

Neither FOIP nor LA FOIP apply to most businesses in the province or non-profit organizations operating in the province. Federal legislation in the *Personal Information Protection and Electronic Documents Act* (PIPEDA) (maybe soon Bill C-27) applies to federally regulated organizations such as banks, railways and airlines. Employees in those organizations would have protection under PIPEDA (or Bill C-27). There are businesses and non-profit organizations in Saskatchewan to which PIPEDA does not apply. All of this means that some employees of businesses and non-profit organizations in the province do not have any protection when it comes to their personal information or personal health information held by their employer.

The Health Information Protection Act (HIPA) was passed in 2003. It applies to a trustee as defined in the act and in the regulations. It generally covers all those organizations that operate in the health sector. It applies to the personal health information held by trustees regarding their patients. If an employee's personal health information is held by a trustee (who is also their employer), then the employee has protection of their personal health information, but no protection of other personal information held by that trustee (employer) unless they are also a local authority or government institution. As a result, there is a segment of employees whose personal information and personal health information is not protected under any of the current legislation.

There are exceptions where the SEA deals with the collection of employee information. I particularly note subsection 2-56.1(7) which provides as follows:

> **2-56.1(7)** If the employer so requires, the employee shall provide written evidence issued by persons identified in subsection 12.4(4) of *The Victims of Interpersonal Violence Act* to verify the circumstances of the leave.

I also note that other sections of the SEA allow employers to ask for medical certificates. For example, in section 2-47, an employer can require medical evidence from a medical practitioner.

Also, in section 2-49 dealing with maternity leave and in subsection (7), the employer can ask for bona fide medical reasons for ceasing work immediately. Finally in section 2-17, subsection (3), the employer can require a medical certificate.

Medical evidence or medical certificates can contain highly sensitive personal information or personal health information about an employee or a family member. For example, it may refer to cancer, HIV, mental illness or pregnancy complications, to name a few. I believe this type of information requires similar protection as provided in subsection 2-56.1(5), which provides as follows:

> **2-56.1**(5) An employer must:
>
> (a) maintain confidentiality respecting all matters that come to the employer's knowledge in relation to leave taken by an employee pursuant to this section; and
>
> (b) not disclose information relating to the leave to any person except:
>
> (i) employees or agents of the employer who require the information to carry out their duties; or
>
> (ii) with the consent of the employee to whom the leave relates.

To summarize, some employees have protections under legislation for their personal information and personal health information, but not all employees have that protection. It is only fair if all employees in the province have basically the same protection regardless of where they work.

Paper to Digital

Our society has shifted from a paper-based society to a digital society. COVID-19 accelerated that trend. Much of people's personal information is stored in a computer somewhere in the province, Canada or internationally. We frequently hear of breaches of computer systems happening in our province, Canada or internationally. All of this has made our personal information vulnerable to misuse by criminal elements. This has increased the need for every employer to take more and more steps to protect the personal information they hold. If an employer is covered by legislation, then there is an expectation and duty to protect that personal information. If an employer is not covered by any of the above referred to legislation, then no legislated duty to protect applies to that employer. That just makes employee information held by that employee more vulnerable. Again, there is a need to have all employees covered by legislation that deals with the collection, use, disclosure and protection of employee's personal information in the province.

Proposals - *The Saskatchewan Employment Act* (SEA)

Most privacy legislation focuses on collection of personal information, use of personal information, disclosure of personal information, access, correction rights and protection of personal information scheme. This submission proposes a new Part X in the SEA that would address each of those issues.

The proposals below combine provisions from PIPEDA, Manitoba's *Personal Information Protection and Identity Theft Prevention Act* and Alberta's and British Columbia's *Personal Information Protection Act.* Everything that follows would be inserted into the SEA as a new Part X.

Interpretation

Before addressing the collection, use, disclosure, and protection proposals, it is necessary to acknowledge that a new Part X in the SEA would have some terms that would need to be defined for the purposes of the new Part. The following terms defined may not be exhaustive and there may be other terms that would need to be defined. The proposal below is a preliminary list of definitions required for the new Part.

Interpretation
10-1 In this Part:

(a) **"business contact information"** means any information that is used for the purpose of communicating or facilitating communication with an individual in relation to their employment, business, or profession such as the individual's name, position name or title, work address, work telephone number, work fax number or work electronic address;

(b) "**commissioner**" means the Information and Privacy Commissioner of Saskatchewan appointed pursuant to *The Freedom of Information and Protection of Privacy Act;*

(c) **"employee"** means an individual employed by an employer and includes a former employee; an individual retained under a contract to perform services for the employer;

(d) "**employee personal information**" means personal information about an individual who is a potential, current or former employee of an employer that is collected, used, or disclosed for the purposes reasonably required to establish, manage, or terminate an employment relationship between the employer and that individual, but does not include personal information that is unrelated to an individual's employment;

(e) "**government institution**" means a government institution as defined in *The Freedom of Information and Protection of Privacy Act* and regulations;

(f) **"information management service provider"** means a person who or body that:

(i) processes, stores, archives, or destroys records of an employer containing employee personal information; or

(ii) provides information management or information technology services to an employer with respect to records of the employer containing employee personal information;

(g) "**local authority**" means a local authority as defined in *The Local Authority Freedom of Information and Protection of Privacy Act* and regulations;

(h) **"personal information**" means information about an identifiable individual, is personal in nature and includes personal health information relating to the individual's physical or mental health or health services received and does not include business contact information;

(i) **"trustee"** means a trustee as defined in *The Health Information Protection Act* and regulations.

Application

This proposal suggests that this new Part would apply to businesses and non-profit organizations operating in Saskatchewan not otherwise covered by the provincial and federal privacy legislation.

Application

10-2 (1) Subject to subsections (2) and (3), this Part applies to every employer with respect to all employee personal information.

(2) This Part does not apply to a government institution or local authority or any personal information, employee or other, in the possession of or under the control of a government institution or a local authority.

(3) This Part does not apply to any trustee with custody or control of personal health information of its employees.

Collection of Employee Personal Information

Essential to the employment relationship is information that the employer needs to collect in order to properly hire, pay, make payroll deductions, approve sick leave and approve other leaves such as domestic violence leave. As employers collect information, it is possible they collect more information than is required for their purposes. As employers collect information regarding employees, it is best practice that employers inform employees that they are collecting such information and inform them of the purpose for which it is being collected. Best practice would dictate that employers collect the least amount of information required to meet their needs.

Collection of employee personal information

10-3(1) Subject to subsection (2), an employer may collect employee personal information with the consent of the employee.

(2) An employer may not collect employee personal information without the consent of the employee unless it is not reasonably practicable to obtain consent and the information is collected solely for the purposes of:

(a) establishing, managing or terminating an employment relationship between the employer and the employee;

(b) managing a post-employment relationship between the organization and the employee; or

(c) complying with a law or regulation.

(3) Where an employer intends to collect employee personal information on all or many employees, it must develop and provide to those employees a policy setting out what employee personal information will be collected, how it will be collected, the purpose for which it is being collected, who will have access to the employee personal information and when the employee personal information will be destroyed.

(4) Nothing in this section is to be construed to restrict or otherwise affect an employer's ability to collect employee personal information otherwise authorized pursuant to this Act or regulations.

Manner of Collection

Manner of collection

10-4 An employer shall, where reasonably practicable, collect employee personal information directly from that employee to whom it relates and provide notice of the purpose of the collection to the employee before or at the time of collection, except where:

(a) the employee authorizes collection by other methods;

(b) doing so could reasonably be expected to compromise the availability or the accuracy of the employee personal information;

(c) collection of the information is reasonable for the purposes of an investigation or legal proceeding; or

(d) the collection of the information is necessary to comply with a collective agreement that is binding on the employer.

Use of Employee Personal Information

Once employers have collected employee personal information, they will have a need to use that information for purposes related to the employment relationship. For example, employers need to supervise and control vacation leave, sick leave and other leaves, and manage accommodations. Best practice would require that employee personal information only be used for that limited purpose. There is also an issue as to who in the organization should have access to that information and who should not.

Use of employee personal information

10-5(1) Subject to subsection (2), an employer may use employee personal information with the consent of the employee.

(2) An employer may use employee personal information without the consent of the employee:

(a) for the purpose for which the information was obtained or compiled, or for a use that is consistent with that purpose;

(b) for a purpose for which the information may be disclosed pursuant to subsection 10-5; or

(c) for the purpose of complying with:

(i) an Act or a regulation; or

(ii) an Act of the Parliament of Canada or a regulation made pursuant to an Act of the Parliament of Canada; or

(d) the information is collected for the purpose of:

(i) management;

(ii) audit; or

(iii) administration of personnel;

by the employer.

(3) Nothing in this section is to be construed as to restrict or otherwise affect an employer's ability to use employee personal information otherwise authorized pursuant to this Act.

(4) Nothing in section is to be construed as authorizing an employer to use or obtain access to the personal health information of an individual who is an employee or prospective employee for any purpose related to workplace accommodation without the individual's consent.

Disclosure of Employee Personal Information

Employers may have to disclose employee personal information to someone outside the organization from time to time. Best practice would be that such disclosures only occur to person's who need-to-know, and disclosures involve releasing the least amount of employee personal information.

Disclosure of employee personal information

10-6 Subject to any other Act or regulation, an employer may disclose employee personal information without consent of the employee only if:

(a) reasonably related to establishing, managing of terminating an employment relationship between the employer and the employee;

(b) related to the management of a post-employment relationship between the employer and the employee;

(c) necessary for the purposes of assisting the employer to determine the employee's eligibility or suitability for a position with that employer;

(d) necessary to respond to an emergency that threatens the life, health, or security of the employee or another individual;

(e) for the purpose of complying with a subpoena, warrant or order issued or made by a court, person, or body with jurisdiction to compel the production of employee personal information;

(f) if the disclosure is necessary to comply with a collective agreement that is binding on the employer;

(g) the disclosure is reasonable for the purposes of an investigation or a legal proceeding;

(h) otherwise permitted under this Act; or

(i) for the purpose of complying with:

(i) a legislative instrument of a professional regulatory organization;

(ii) an Act or a regulation; or

(iii) an Act of the Parliament of Canada or a regulation made pursuant to an Act of the Parliament of Canada.

Access

As employers collect employee personal information, the employee should have the right to find out what the employer has collected. Best practice would give the employee a right of access subject to some exceptions.

Access

10-7(1) Subject to subsections (2) to (3), on the request of an employee for access to employee personal information about the employee and taking into consideration what is reasonable, an employer must provide the employee with access to the employee's personal information, where that information is contained in a record that is in the possession or under the control of the employer, the request is made in writing and includes sufficient detail to identify.

(2) An employer may refuse to provide access to employee personal information under subsection (1) if:

(a) the information is protected by any legal privilege including solicitor-client privilege;

(b) the disclosure of the information would reveal confidential information that is of a commercial nature, and it is not unreasonable to withhold that information;

(c) the information was collected for an investigation or legal proceeding;

(d) the information was collected by a mediator or arbitrator or was created in the course of a mediation or arbitration for which the mediator or arbitrator was appointed to act:

(i) under an agreement;

(ii) under an enactment; or

(iii) by a court; or

(e) the information relates to or may be used in the exercise of prosecutorial discretion.

(3) An employer shall not provide access to employee personal information under subsection (1) if:

(a) the disclosure of the information could reasonably be expected to threaten the life or security of the employee or another individual;

(b) the information would reveal personal information about another individual; or

(c) the information would reveal the identity of an individual who has in confidence provided an opinion about the employee and the individual providing the opinion does not consent to disclosure of his or her identity.

(4) An employer must respond to an employee not later than 30 days from the day the organization receives the employee's written request.

(5) The failure of an employer to respond to the request within the legislated timeline is to be treated as a decision to refuse the request.

Information Management Service Provider

Many employers contract with information management service providers to provide computer and system services to the employer. This could include contracting a vendor to provide payroll management services. By providing the service provider with employee personal information, the employer is disclosing that information outside its organization. Although such arrangements are generally necessary, it is important that the employer ensure that the service provider will act properly and protect the employee personal information.

Information management service provider

10-8(1) An employer may provide an employee personal information to an information management service provider for the purposes of:

(a) having the information management service provider process, store, archive or destroy the employee personal information for the employer;

(b) enabling the information management service provider to provide the employer with information management or information technology services;

(c) combining records containing employee personal information; or

(d) providing consulting services.

(2) Before providing employee personal information to an information management service provider, an employer must enter into a written agreement with the information management service provider that:

(a) governs the access to and use, disclosure, storage, archiving, modification, and destruction of the employee personal information; and

(b) provides for protection of the employee personal information.

(3) An information management service provider shall not obtain access to, use, disclose, process, store, archive, modify or destroy employee personal information received from an employer except for the purposes set out in subsection (1).

(4) An information management service provider must comply with the terms of the written agreement entered into pursuant to subsection (1).

(5) For the purposes of subsection (1), a written agreement that is entered into between an employer and an information management service provider must include:

(a) a description of the specific service the information management service provider will deliver;

(b) provisions setting out the obligations of the information management service provider respecting the security and safeguarding of the employee personal health information;

(c) provisions for the destruction of the employee personal health information, if applicable;

(d) a requirement that the information management service provider not use, disclose, obtain access to, process, store, archive, modify or destroy employee personal health

information received from an employer except for the purposes set out in subsection (1);

(e) a requirement that the information management service provider comply with the terms of the written agreement entered into with the employer; and

(f) a requirement that the information management service provider notify the employer at the first reasonable opportunity of any breach of the agreement.

Fees

Employers have collected information about employees, and it is only fair that the employee have access to that information without any barriers or obstacles.

Fees

10-9 An organization shall not charge a fee in processing and providing records responsive to a request by an employee for that employee's personal information.

Right to Request Correction

As employers collect employee personal information, it is possible that they collect information with errors. Best practice would be to allow an employee to make a request for collection.

Right to request correction

10-10(1) An employee may request that an employer correct an error or omission in that employee personal information that is in the possession or under the control of the employer.

(2) If there is an error or omission in the employee personal information in respect of which a request for correction is received by an employer under subsection (1), the employer, subject to subsection (2),

(a) correct the information as soon as reasonably practicable; and

(b) where the employer has disclosed the incorrect information to other employers, send a notification containing the corrected information to each employer to which the incorrect information has been disclosed, if it is reasonable to do so.

(3) If an employer is satisfied on reasonable grounds that a requested correction under subsection (2) should not be made, the employer must annotate the employee personal information under its control with the correction that was requested but not made.

Protection of Employee Personal Information

As employers collect employee personal information, it is only fair that they are obliged to protect that information. The employee personal information needs to be protected from unauthorized breaches by other employees and unauthorized breaches from outsiders and other bad actors.

Protection of employee personal information

10-11 An employer must protect employee personal information in its possession or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks.

Notification

In today's society, it is not "if a breach of an employer will occur", but "when a breach will occur". When a breach occurs, it is necessary that the employer take steps to notify the persons affected. It is only when a person is informed of a breach of their employee personal information that they can take steps to mitigate the risks of the breach. Breaches may involve unauthorized access to an employee's home address, SIN, bank account number or Visa card number. This type of information can be used to create a false identity and used to commit fraud. Best practice dictates that an employee be made aware of the breach.

Notification

10-12 An employer shall take all reasonable steps to notify an employee or former employee of an unauthorized use or disclosure of that employee's personal information if it is reasonable in the circumstances to believe that the incident creates a real risk of significant harm to the employee.

Employee Personal Information of Deceased Employee

Employees resign or retire, and many employers would retain their employee personal information for some time, the question is for how long. In other legislation, 25 years has been used with an exception for compassionate reasons.

Employee personal information of deceased employee

10-13(1) Subject to subsection (2) and to any other Act, the employee personal information of a deceased employee or former deceased employee shall not be disclosed until 25 years after the death of the employee or former employee.

(2) Where, in the opinion of the employer, disclosure of the employee or former employee personal information of a deceased employee or former employee to the employee's next of kin would not constitute an unreasonable invasion of privacy, the employer may disclose

that employee or former employee, employee personal information before 25 years have elapsed after the employee's or former employee's death.

Rights Exercised by Others

When an employee dies, the executor or administrator may require information to properly administer the employee's estate. Similarly, when an employee has a property guardian, the property guardian many require information from the employer. Finally, when an employee appoints an attorney under a power of attorney, the attorney may require information from the employer.

Exercise of rights by other persons

10-14 Any right or power conferred on an employee by this Act may be exercised:

(a) where the employee is deceased, by the employee's personal representative if the exercise of the right or power relates to the administration of the employee's estate;

(b) where a personal guardian or property guardian has been appointed for the employee, by the guardian if the exercise of the right or power relates to the powers and duties of the guardian;

(c) where a power of attorney has been granted by the employee, by the attorney if the exercise of the right or power relates to the powers and duties of the attorney conferred by the power of attorney;

(d) where the employee is less than 18 years of age, by the employee's legal custodian in situations where, in the opinion of the employer, the exercise of the right or power would not constitute an unreasonable invasion of the privacy of the employee; or

(e) by any person with written authorization from the employee to act on the employee's behalf.

Conduct of Reviews and Investigations

As indicated above, employees would have the right to request their employee information or the right to correction of information but when they do so, employers may decline their request or only provide part of the information requested. In addition, employers might improperly use or disclose information of an employee or a group of employees. In order to make the system work it is necessary to have a place where employees unhappy with what has occurred can complain or appeal. The Information and Privacy Commissioner of Saskatchewan is set up to investigate complaints of refusal to provide information or investigate improper use or disclosure of information. The proposal below gives the Information and Privacy Commissioner of Saskatchewan the authority to review and investigate.

Conduct of Reviews and Investigations

10-15(1) If the commissioner considers it appropriate to do so, the commissioner may conduct an investigation or a review of a decision made by an employer pursuant to this Part.

(2) Section 33 and Part VII of *The Freedom of Information and Protection of Privacy Act* applies, with any necessary modification, to the conduct of an investigation or review by the commissioner under this Part.

Retention and Destruction of Employee Personal Information

Employers need to collect employee personal information to make the employment relationship work properly. There is a point when the employee personal information is no longer needed. For example, after a certain number of years after an employee retires or resigns, there will be other instances where employee personal information collected does not have to be kept until the employee retires or resigns. For example, when recruiting for a position, resumes of individuals who did not get the job may not to be kept for very long. The needs of each employer will be different in terms of what is kept and for how long it is kept. But the important point is that some day the employee personal information can be destroyed. An employee should know how long their employee personal information will be kept. It is reasonable to expect the employer have a policy on this matter.

Retention and destruction policy

10-16(1) An employer must:

(a) have a written policy concerning the retention and destruction of employee personal information that meets the requirements set out in the regulations; and

(b) comply with that policy and any prescribed standards with respect to the retention and destruction of employee personal information.

(2) An employer must ensure that:

(a) employee personal information stored in any format is retrievable, readable and useable for the purpose for which it was collected for the full retention period of the information established in the policy mentioned in subsection (1); and

(b) employee personal information is destroyed in a manner that protects the privacy of the employee.

Conclusion

In conclusion, I would ask that those responsible for the Employment Standards Review consider the recommendations and proposals that a new Part X be added to the SEA, which

would deal with the collection, use, disclosure and protection of employee personal information held by businesses and non-profit organizations in the province.

If you have any questions, please feel free to contact me at 306 537-4287.

All of which is respectfully submitted this 28th day of September 2023.

Ronald J. Kruzeniski, K.C.
Saskatchewan Information and Privacy Commissioner
rkruzeniski@oipc.sk.ca