ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

ORDER F2019-05

March 8, 2018

ALBERTA HUMAN RIGHTS COMMISSION and JUSTICE AND SOLICITOR GENERAL

Case File Numbers 000814 and 011306

Office URL: www.oipc.ab.ca

Summary: The Complainant was employed as legal counsel for the Alberta Human Rights Commission (AHRC); his employment ended in 2014. The Complainant states that he left his workplace immediately after his employment ended. He states that he was told his personal files would be collected and returned to him. However, he states that these items have not been returned and that he was told they were subject to a review by his employer.

The Complainant made a complaint to this Office that AHRC had contravened the *Freedom of Information and Protection of Privacy Act* by collecting, using and/or disclosing his personal information in his personal files.

Subsequent to the investigation conducted by this Office, the Complainant requested an inquiry into AHRC's actions. Justice and Solicitor General (JSG) was added as a party.

The Adjudicator found that AHRC did not collect the Complainant's personal information by virtue of his placing it on AHRC premises, computers or network environment. She found that AHRC also did not collect the Complainant's personal information when it gathered up the Complainant's files and provided them to JSG. Because AHRC did not collect the Complainant's personal information, it follows that AHRC did not use or disclose it. The Adjudicator determined that AHRC also did not have a duty to make reasonable security arrangements to protect that information.

The Adjudicator found that JSG did not collect the Complainant's personal information when it took possession of the Complainant's gathered files or when it reviewed the files for the sole purpose of determining which records 'belonged' to JSG and which 'belonged' to the Complainant. However, the Adjudicator determined that JSG collected the personal information in the files when it retained the files for its own purposes.

The Adjudicator accepted that JSG's reasons for collecting the personal information were to manage the Complainant's employment relationship, specifically his termination, and respond to allegations made by the Complainant in various legal proceedings related to his termination. The Adjudicator found that the collection was authorized under section 33(c) of the Act.

The Adjudicator found that JSG used the personal information for the same purposes for which it was collected (section 39(1)(a) and 41).

The Adjudicator determined that JSG had a duty to make reasonable security arrangements to protect the personal information. She found that the measures taken by the Public Body to secure the information met this duty.

Statutes Cited: AB: *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25, ss. 1, 33, 38, 39, 40, 41, and 72, *Personal Information Protection Act*, S.A. 2003, c. P-6.5, s. 4

Authorities Cited: AB: Investigation Report F2015-IR-001, Orders F2005-003, F2009-023, F2009-048, F2013-31, F2015-27, F2016-19, F2018-37, **ON**: Order MO-2408

Cases Cited: *Alberta Child Welfare v. C.H.S.*, 2005 ABQB 695 (CanLII), *City of Ottawa v. Ontario*, 2010 ONSC 6835, *University of Alberta v. Alberta (Information and Privacy Commissioner)*, 2012 ABQB 247

I. BACKGROUND

[para 1] The Complainant was employed as legal counsel for the Alberta Human Rights Commission (AHRC); his employment ended in 2014.

[para 2] The Complainant states that he left his workplace immediately after his employment ended. He states that he was told his personal possessions and pro bono files would be collected and returned to him. However, he states that these items have not been returned and that he was told they were subject to a review by his employer.

[para 3] On April 15, 2015, the Complainant made a complaint to this Office that AHRC had contravened the *Freedom of Information and Protection of Privacy Act* by collecting, using and/or disclosing his personal information. Specifically, the Complainant states in his complaint:

> The collection, refusal to return, inspection, review and improper safeguarding of my personal belonging[s], pro bono files breaches my privacy as well as the solicitor-client privilege.

[para 4] The Complainant lists the personal belongings as

> family pictures, personal files, health records, personal research, education documents, pro bono files and other personal information that has nothing to do with my employment. These files were kept secure on a designated personal folder, which I was allowed to use for my private use. These included information about current health issues and personal medical prescriptions.

[para 5] Mediation was authorized but did not fully resolve the issues between the parties and on July 24, 2016, the Complainant requested an inquiry. I received submissions from both parties.

[para 6] In the course of the inquiry, Justice and Solicitor General (JSG) requested that it be added as an affected party on this inquiry. It provided a copy of a decision of the Alberta Court of Appeal in connection with a related legal proceeding, which affirmed that while the Complainant was counsel to AHRC, he was employed by JSG. JSG argued that the post-termination actions at issue in this inquiry involved both AHRC and JSG.

[para 7] I have reviewed the case provided by JSG. It is clear that the Minister of Justice and Solicitor General has the authority to appoint and terminate counsel for AHRC. I agreed to add JSG as an affected party to the inquiry.

[para 8] Submissions for AHRC were made by the JSG FOIP unit on AHRC's behalf. As they were made on AHRC's behalf, I will refer to them as AHRC's submissions. The submissions relate to both AHRC's actions and those of JSG with respect to the collection, use, and disclosure of personal information, as well as security arrangements. JSG did not make separate submissions once it was added as a party.

[para 9] After reviewing the submissions and considering the issues, I informed the parties that JSG would be added to the inquiry as a 'full' party (letter dated January 28, 2019). I had determined that my findings regarding the issues in the inquiry may extend beyond whether AHRC did or did not contravene the FOIP Act; they may also include a finding that AJSG did or did not contravene the FOIP Act. The parties were provided with an opportunity to make further submissions based on this change to the inquiry; none did.

[para 10] As this inquiry now addresses the actions of two public bodies, I will refer to AHRC and JSG rather than "the Public Body".

[para 11] File number 000814 refers to the file initially opened up by this Office with respect to the complaint about AHRC. During the inquiry, this Office created file number 011306 to track any decisions made in this inquiry with respect to JSG. This new file number is relevant only to the internal record keeping of this Office.

II. ISSUES

[para 12] The Notice of Inquiry dated April 17, 2018 states the issues in this inquiry as follows:

1. Did the Public Body collect the Complainant's personal information?

This question is to decide if the Public Body's access of the information on its premises or in its electronic systems for the purpose of review to determine its ownership was a "collection" within the terms of the Act, and if the information collected was the Complainant's "personal information".

2. If yes, did it do so in compliance with or in contravention of section 33 of the Act?

3. Did the Public Body use the Complainant's personal information? If yes, did it have authority to do so under sections 39(1) and 39(4) of the Act?

4. Did the Public Body disclose the Complainant's personal information? If yes, did it have authority to do so under sections 40(1) and 40(4) of the Act?

This includes any disclosure to another public body to review any personal information of the Complainant.

5. Did the Public Body meet its obligations as required by section 38 of the Act (protection of personal information)?

This question is meant to address the Complainant's concern about the absence of a policy for dealing with an employee's personal records on termination.

[para 13] In his complaint, request for inquiry, and submission to the inquiry, the Complainant has referred to both the FOIP Act and to the *Personal Information Protection Act* (PIPA). PIPA applies to private-sector organizations; it does not apply to public bodies that are subject to the FOIP Act (section 4(2) of PIPA). Both JSG and AHRC are public bodies under the FOIP Act and therefore PIPA is not relevant to this inquiry. To the extent that the Complainant's arguments regarding PIPA are relevant to the collection, use and/or disclosure of personal information under the FOIP Act, I will consider them.

III. DISCUSSION OF ISSUES

1. Did AHRC and/or JSG collect the Complainant's personal information?

[para 14] Under this issue, the Notice of Inquiry states:

> *This question is to decide if the Public Body's access of the information on its premises or in its electronic systems for the purpose of review to determine its ownership was a "collection" within the terms of the Act, and if the information collected was the Complainant's "personal information".*

[para 15] The parties have also addressed whether JSG collected the Complainant's personal information.

[para 16] With its submission, AHRC provided an affidavit sworn by an Employee Relations Advisor of JSG. The Advisor states that she was advised (Tab 8, at para 2):

a. all tangible personal effects, including personal photographs, files, magazines, personal books, loose paper, including any records containing [the Complainant's] health information and prescription information, that were physically located in [the Complainant's]former office were returned to him in 17 boxes and one briefcase that were delivered to [the Complainant] on December 22, 2014,
b. all tangible items in [the Complainant's] office were sorted, boxed, sealed and returned and only a general inventory list was created, and,
c. the only physical files that were retained were files containing Alberta Human Rights Commission work product. Unless part of a file contained Alberta Human Rights Commission work product, any loose papers or photocopies found in [the Complainant's] office were returned to him in the 17 boxes and one briefcase that were delivered to him.

[para 17] AHRC also provided a copy of an affidavit sworn by a Manager of Employee Relations with JSG for a judicial review proceeding relating to the Complainant's termination. The Manager states in that affidavit that the electronic records located on the Complainant's government employee profile amounted to over 21 gigabytes of information comprising approximately 214, 151 separate records, including emails and attachments. The Manager states that these files must be reviewed and sorted before the 'purely personal' items could be provided to the Complainant (Tab 8, appendix A, at para. 4).

[para 18] AHRC states that many of the items referred to by the Complainant as being collected by AHRC are not his personal information. Of the items listed by the Complainant in his complaint (cited at para. 4 of this Order), AHRC states the following include or may include his personal information:

- family pictures,
- possibly personal files (only if they contain The Complainant's personal information),
- possibly health records (only if they are the Complainant's health records), and
- possibly personal medical prescriptions (only if the prescriptions are the Complainant's prescriptions).

[para 19] AHRC further argues that the personal research, education documents and pro bono files do not contain his personal information, or contain very little.

[para 20] Personal information is defined in section 1(n) of the Act as follows:

> *1(n) "personal information" means recorded information about an identifiable individual, including*
>
> > *(i) the individual's name, home or business address or home or business telephone number,*
> >
> > *(ii) the individual's race, national or ethnic origin, colour or religious or political beliefs or associations,*

> *(iii) the individual's age, sex, marital status or family status,*
>
> *(iv) an identifying number, symbol or other particular assigned to the individual,*
>
> *(v) the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics,*
>
> *(vi) information about the individual's health and health care history, including information about a physical or mental disability,*
>
> *(vii) information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given,*
>
> *(viii) anyone else's opinions about the individual, and*
>
> *(ix) the individual's personal views or opinions, except if they are about someone else;*

[para 21] All parties accept that some of the records contain the Complainant's personal information. Some of the records are in hardcopy format and some are electronic. In its submission, AHRC has referred to hardcopy records (and other personal effects, which are not relevant to this inquiry) as 'tangible' records. For ease of reference I will adopt AHRC's terminology.

[para 22] From the submissions it seems likely that the tangible records included records containing the Complainant's personal information. AHCR's submissions also refer to the electronic records as containing the Complainant's personal information (e.g. at page 12).

[para 23] Some records, such as pro bono files, are less likely to contain the Complainant's personal information. These files presumably contain the Complainant's work product as counsel to parties other than AHRC. Work performed by the Complainant – whether for AHRC or a third party – is generally not characterized as personal information unless it has a personal dimension. I do not have copies of any of the information in these pro bono files, nor any specifics regarding the information.

[para 24] Similarly, personal research may not contain the Complainant's personal information. The fact that the Complainant performed the research does not make it his personal information, especially if it was research related to his role as counsel for third parties. That said, the Complainant may have researched personal matters, such as vacation plans, medical diagnoses, or other issues unrelated to his work, which might have a personal dimension.

[para 25] Based on the somewhat limited information before me, I conclude that at least some of the tangible records and some of the electronic records contain the Complainant's personal

information. Some tangible records and some electronic records likely do not contain the Complainant's personal information. This Order concerns only the records that contain the Complainant's personal information.

[para 26] I will further note that it seems likely that the personal information of individuals other than the Complainant is contained in the records – the family photos are the most obvious instance. The personal research, personal documents, pro bono files etc. may also include third party personal information. However, a complainant can request a review of a public body's collection, use and/or disclosure only of their own personal information (section 65(3)). Therefore, the scope of this inquiry addresses only the collection, use and/or disclosure of the Complainant's own personal information, even if third party personal information is contained in the records.

Did AHRC or JSG collect the Complainant's personal information?

[para 27] AHRC states that it did not collect the Complainant's personal information. Rather, it argues (at page 5):

> he independently collected and stored his personal information, as well as other information (*i.e.* files relating to his "pro bono" work) on Government servers. [The Complainant] independently and voluntarily placed his personal information on Government servicers. To the extent that accessing [the Complainant]'s personal information post-termination – information that he had personally placed on Government servers – was a collection of that information, it was authorized under FOIP in order to manage or administer personnel of the Government of Alberta.

[para 28] The Complainant did not respond to AHRC's arguments on this point.

[para 29] Section 33 of the FOIP Act places strict limits on personal information a public body can collect. It states:

> *33 No personal information may be collected by or for a public body unless*
>
> *(a) the collection of that information is expressly authorized by an enactment of Alberta or Canada,*
>
> *(b) that information is collected for the purposes of law enforcement, or*
>
> *(c) that information relates directly to and is necessary for an operating program or activity of the public body.*

[para 30] AHRC states that it is arguable that the personal information placed on the government servers by the Complainant is not personal information to which the FOIP Act applies. It cites Order F2016-19, *University of Alberta v. Alberta (Information and Privacy Commissioner)*, 2012 ABQB 247 (*University of Alberta*) and *City of Ottawa v. Ontario*, 2010 ONSC 6835 (*City of Ottawa*) in support of this position.

[para 31] In Order F2016-19, the adjudicator considered a public body's response to an access request for emails and texts between city councilors. The applicant specified that they were

seeking personal and professional emails/texts. The adjudicator states that it is unclear whether personal emails/texts would be within the custody and control of a public body in the sense that it does not have a legal right to demand those emails/texts. She said that personal emails and texts that are not created in an employee's representative capacity may not be records over which the FOIP Act applies. Ultimately the adjudicator did not have to make a decision on that issue.

[para 32] *City of Ottawa* is a decision of the Ontario Superior Court, resulting from a judicial review of Order MO-2408 of the Ontario Information and Privacy Commissioner. In that case, an employee of the city had used his city work email account to send and receive emails relating to his volunteer role with another organization. An access request was made for those emails. The adjudicator in Order MO-2408 found that the emails were in the custody or control of the city because the city had physical custody of emails on its server and also had control to regulate its email system. The Court overturned that decision.

[para 33] The Court reviewed the ten factors considered by the Ontario adjudicator in determining whether the city had control over the personal emails. These factors are the same as the ten factors used in past Orders of this Office in determining control over records (see Order F2016-19 at para. 17). The Court considered these factors in the context of the purpose of the access-to-information provisions in the Act, which is to facilitate democracy. It concluded that the city did not have custody such that the personal emails could be the subject of an access request. Applying the factors, the Court noted that while the city employee created some of the records, the records were not created in the course of his work duties. Other records were sent to the employee by an individual unrelated to the city. These records were not intended to be used for city business, and were not related to city business. The city *did* possess the records by virtue of the employee's use of the city email system but it did not have a *right* to possess the records. The city had some ability to regulate the record because it regulates its email system and the record was on the system. The city did not have the ability to regulate the record itself, outside of that email system.

[para 34] The Court also noted that it is not uncommon for employees to have or bring personal paper documents to their workplace. It stated that electronic documents are not different in this regard. It said (at paras. 37-38):

> It can be confidently predicted that any government employee who works in an office setting will have stored, somewhere in that office, documents that have nothing whatsoever to do with his or her job, but which are purely personal in nature. Such documents can range from the most intimately personal documents (such as medical records) to the most mundane (such as a list of household chores). It cannot be suggested that employees of an institution governed by freedom of information legislation are themselves subject to that legislation in respect of any piece of personal material they happen to have in their offices at any given time. That is clearly not contemplated as being within the intent and purpose of the legislation.
>
> The question then is whether information stored electronically should be treated any differently. I do not see any rational basis for making such a distinction.

[para 35] The Ontario Court discussed the fact that electronic records (unlike paper or tangible records) were subject to the city's "Responsible Computing Policy", which stated that the city

had the right to access its IT assets and information, and to monitor their use. The Court found that this management of IT services did not amount to custody or control of the personal emails of the city employee, located on the city's servers. The Court noted (at para. 42):

> Employers from time to time may also need to access a filing cabinet containing an employee's personal files. That does not make the personal files of the employee subject to disclosure to the general public on the basis that the employer has some measure of control over them. The nature of electronically stored files makes the need for monitoring more pressing and the actual monitoring more frequent, but it does not change the nature of the documents, nor the nature of the City's conduct in relation to them. It does not, in my view, constitute custody by the City, within the meaning of the Act.

[para 36] This Ontario decision is cited by the Alberta Court of Queen's Bench in *University of Alberta*, a decision resulting from a judicial review of Order F2009-023. The Order related to whether the University had custody or control of emails sent or received by a professor in connection with his voluntary participation in a grant process for a federal program. The Court found that the professor's emails were akin to the city employee's personal emails in *City of Ottawa*, and that the University did not have custody or control over them. It noted that the University's ability to monitor emails on its server and its Condition of Use policy did not indicate it had custody or control. The Court also noted that the University's duty to maintain the security of its email system did not mean it has custody or control over all emails contained in that system.

Application to Part 2 of the Act

[para 37] Custody and control are terms that arise only occasionally in inquiries regarding complaints under Part 2 of the Act. These terms did arise in Order F2018-37, in which the adjudicator considered whether the duty to make reasonable security arrangements under section 38 applies where the public body did not have custody or control of the personal information at issue. I will discuss that Order in issue #5.

[para 38] The *University of Alberta* and *City of Ottawa* cases relate to access to information under Part 1 of the Act but are nevertheless informative in this case. Specifically of use are the discussions regarding whether a public body has control over personal records (tangible or electronic) brought into the workplace by employees.

[para 39] It is not unusual for an employee to keep personal information at their workplace, such as family photos, diplomas and certificates, and medical information to be submitted for health benefits. Where an employee brings such information into the workplace and files it in a desk drawer or tacks it on a bulletin board, a public body might be characterized as having 'custody' of such items insofar as they are on a public body's premises.

[para 40] However, a public body as employer generally does not have authority to 'collect' such personal information under section 33. Were section 33 to apply in these circumstances, public bodies would have to prohibit personal items or risk contravening section 33 of the Act. Such a result seems nonsensical.

[para 41] Electronic copies of records have additional considerations not arising where the personal information is in a tangible record sitting in or on a desk. Public bodies have obligations to maintain and monitor electronic systems such as email servers and document storage. They also have terms of use policies that employees must abide by. Personal documents (such as photos) uploaded onto a public body's network by an employee can be included in scans conducted by the public body to locate malware etc. on its systems. Those personal documents could be quarantined or deleted by the public body if necessary to maintain security of its systems. A public body could even decide to mass-delete items saved on its servers, or wipe a computer hard drive to contain malware etc.

[para 42] However, a public body could also empty its physical location. In all of these situations, the public body has the ability to delete or remove items containing employee personal information that the employee has brought into the workplace and/or uploaded to a computer or network. Therefore, the public body has some control over the information whether it is tangible or electronic. This control arises from a public body's duty to maintain its premises, property and systems.

[para 43] The Ontario and Alberta courts have concluded that this ability to regulate personal documents or records by virtue of obligations to maintain its systems is not sufficient, by itself, to give a public body control over these documents such that they can be subject to access requests. As these Courts have stated, the ability to regulate personal documents stems from the public body's ability to regulate its systems and use of its systems. The ability to regulate is not tied to the document itself. Absent other considerations, the public body does not have the right to possess the document or regulate the document other than to maintain its systems. (Other considerations include workplace investigations during which a public body might intentionally collect an employee's personal files kept on the public body premises or electronic system).

[para 44] In my view, this kind of custody or control also does not mean that a public body has collected the personal information within the terms of Part 2 of the FOIP Act. Whether electronic or tangible, when an employee voluntarily stores personal information at the workplace and that information:

- is for the personal use of the employee
- is unrelated to the employee's work duties, and
- is unrelated to the functions of the public body (i.e. is not personal information of the employee collected for human resources purposes)

then the public body will generally not be found to have collected it within the terms of Part 2 of the Act.

[para 45] For these reasons, I agree with AHRC that it did not collect the Complainant's personal information simply by virtue of the fact that the Complainant filed the tangible information in his office and/or saved electronic copies on his work computer or network.

[para 46] I also find that AHRC did not collect the Complainant's personal information when it gathered the tangible records, electronic records and electronic equipment (laptop and iPhone)

and provided them to JSG human resources. Gathering personal effects together, whether putting tangible items into a box or saving electronic copies to a USB stick, is not a collection of the personal information contained in the records.

[para 47] Had JSG taken possession of the records from AHRC for the sole purpose of delivering them to the Complainant, I would have found that it also did not collect the records within the terms of Part 2 of the FOIP Act.

[para 48] In this case, JSG did not merely take possession of the records. It also reviewed the records to separate the Complainant's personal effects from work-related documents. In the affidavit provided by AHRC, an Employee Relations Advisor with JSG states that she was advised by a JSG lawyer that the electronic records at issue were named inconsistently and disorganized such that "it was not possible to rely on the name of an electronic file or its location to determine if the file was personal or work-related" (tab 8, at para. 9c). Therefore, JSG could not simply return the personal files; it was required to review the files to determine which 'belonged' to the Complainant and which 'belonged' to JSG (or AHRC).

[para 49] In Order F2009-048, I found that reviewing records for the purpose of determining their appropriateness for disclosure is not a 'use' of personal information in those records (see paras. 40-42). In that case, the public body had already collected the personal information for human resources purposes. The public body later reviewed those records to determine their appropriateness for disclosure for a different purpose.

[para 50] In my view, reviewing records to determine which 'belong' to the Public Body and which do not is not a 'collection' of that information. This outcome is consistent with my findings above regarding the scope of 'collection' under Part 2 of the Act; it is also consistent with the scope of 'use', discussed in Order F2009-048.

[para 51] In other words, JSG did not collect the Complainant's personal information when it reviewed the documents to determine which to give to the Complainant (as they were his personal effects) and which to keep (as work product properly belonging to JSG or AHRC).

[para 52] That said, I find that JSG *did* collect the Complainant's personal information when it decided to retain the information for its own purposes.

[para 53] In its submissions, AHRC states that upon review of the Complainant's files, JSG discovered that it had cause to terminate the Complainant's employment ("after-acquired" cause). AHRC also states that during its review of the Complainant's files

> … JSG staff discovered the extent of [the Complainant's] misuse of Government resources, and also when [the Complainant] began his various forms of legal proceedings. Thus, the Public Body at that time also used this property and information – of which a portion was [the Complainant's] personal information – in relation to [the various legal proceedings]. (At page 18, emphasis added)

[para 54] AHRC has acknowledged that some of the information in the Complainant's files that was later used in the legal proceedings was the Complainant's personal information. Even if

these files contain very little personal information, quantity does not determine whether the Act applies.

[para 55] I find that JSG collected the Complainant's personal information in his files when it retained some files for its own purposes.

2. If yes, did AHRC and/or JSG do so in compliance with or in contravention of section 33 of the Act?

[para 56] AHRC's submission states that JSG retained the Complainant's personal information in his files for the purpose of managing the employment relationship and responding to allegations made in the course of related legal proceedings.

[para 57] Past Orders of this Office have found that managing personnel of a public body falls within the scope of section 33(c) of the Act (see Orders F2005-003 and F2013-31). The submission from AHRC includes various documents (such as a statement of claim, statement of defence, affidavits and court orders) that show the legal proceedings were related to the Complainant's termination.

[para 58] The Alberta Court of Queen's Bench has considered the use of clients' personal information by a public body in the course of a civil proceeding to be a use as contemplated by section 39(1) of Alberta's Act. In *Alberta Child Welfare v. C.H.S.*, 2005 ABQB 695 (CanLII) (*Child Welfare*), the Court asked whether Alberta Children's Services was entitled to use personal information in its records to defend a lawsuit against it. The Court stated, with respect to consistent use under section 39(1)(a):

> Where files are assembled as a part of a government activity, and litigation arises from that activity, *the use of the information to defend or prosecute* the litigation has a reasonable and direct connection to the purpose for which the information was collected (at para. 24, my emphasis).

[para 59] In my view, a similar statement can be made about the collection of personal information. Legal proceedings arose from the manner in which JSG managed (and terminated) an employment relationship with the Complainant. A public body can collect personal information as necessary to manage an employment relationship under section 33(c). This extends to legal proceedings directly connected to the management of that relationship.

[para 60] I conclude that AHRC did not collect the Complainant's personal information. JSG collected the Complainant's personal information that it retained for the purpose of managing the Complainant's termination, including the related legal proceedings. That collection was authorized under section 33(c) of the Act.

3. Did AHRC and/or JSG use the Complainant's personal information? If yes, did it have authority to do so under sections 39(1) and 39(4) of the Act?

[para 61] Use of the Complainant's personal information is governed by section 39 of the Act. The relevant portions of section 39 of the Act state:

39(1) A public body may use personal information only

> *(a) for the purpose for which the information was collected or compiled or for a use consistent with that purpose,*
>
> *(b) if the individual the information is about has identified the information and consented, in the prescribed manner, to the use, or*
>
> *(c) for a purpose for which that information may be disclosed to that public body under section 40, 42 or 43.*

…

(4) A public body may use personal information only to the extent necessary to enable the public body to carry out its purpose in a reasonable manner.

[para 62] I have found that AHRC did not collect the Complainant's personal information. For the same reasons, I find that it did not use the Complainant's personal information.

[para 63] I found that JSG did collect some of the Complainant's personal information; specifically the information retained to manage the Complainant's termination (including related legal proceedings).

[para 64] AHRC's submissions argue that JSG was authorized to use the Complainant's personal information for the same purpose for which it was collected: manage the termination and for related legal proceedings. It argues that the use was authorized under section 39(c) "cross referenced with section 40(1)(x)" (disclosure for the purpose of managing or administering personnel).

[para 65] Section 39(1)(c) is an oddly-constructed provision and its meaning is not clearly apparent. Not many past Orders of this Office have considered its application. Service Alberta's Guidelines and Practices Manual (2009) explains the provision as follows (at page 263, emphasis added):

> This provision permits a public body to use personal information *that has been disclosed to it* by another public body under section 40, 42 or 43 of the Act.

[para 66] This interpretation was adopted in Investigation Report F2015-IR-01, at paragraph 45:

> I understand section 39(1)(c) to mean a public body is authorized to use personal information it has received from another public body for the purpose for which that information was disclosed to it by the other public body. The public body disclosing the information must have authority under section 40, 42 or 43 to disclose the information.

[para 67] That Investigation Report also referred to Order F2015-27 in support of this position. At paragraph 37 of that Order the adjudicator said:

> For the reasons I have already given, I do not believe this use was authorized under section 39(1)(a), nor do I believe the Complainant gave his consent for this use within the terms of section 39(1)(b). Neither does section 39(1)(c) (use for a purpose for which the information may be disclosed to the public body under section 40) apply, since most of the sub-clauses of section 40 on which the Public Body relies do not authorize disclosure *to* the Public Body. The one that does authorize disclosure to the Public Body (section 40(1)(q)) does not apply, since the DDO's use of the information that had already been collected and compiled in the database was not for the purposes specified in subclauses (i) and (ii) of that provision.

[para 68] The citations from the Guidelines and Practices Manual and the Investigation Report indicate that in order for section 39(1)(c) to apply, the information must have been disclosed to the public body under section 40 of the Act. However, I found that AHRC did not *collect* the Complainant's personal information for the purposes of the FOIP Act and therefore it cannot be said to have *disclosed* the personal information to JSG, within the terms of section 40(1) (for additional discussion on this point, see issue #4 in this Order).

[para 69] Order F2015-27 suggests that in order for section 39(1)(c) to be applicable, the relevant disclosure provision in sections 40, 42 or 43 must authorize disclosure to the specific public body using the information. For example, section 40(1)(q), cited in that Order, authorizes disclosure to a specific type of body (law enforcement).

[para 70] Given the above, it is not clear that section 39(1)(c) authorized the use of the Complainant's personal information by JSG, by reference to section 40(1)(x). However, since AHRC's submissions state that JSG used the information for the same purpose as it was collected by JSG, section 39(1)(a) is applicable. That provision authorizes a public body to use personal information for the purpose for which it was collected, or a consistent purpose.

[para 71] Section 41 of the Act outlines what is meant by consistent purpose as that terminology is used in section 39 of the Act. Section 41 of the Act states:

> *41 For the purposes of sections 39(1)(a) and 40(1)(c), a use or disclosure of personal information is consistent with the purpose for which the information was collected or compiled if the use or disclosure*
>
> > *(a) has a reasonable and direct connection to that purpose, and*
> >
> > *(b) is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses or discloses the information.*

[para 72] I agree that JSG's use of the Complainant's personal information was for the same purpose for which it was collected. Therefore, it was authorized under section 39(1)(a).

[para 73] Finally, pursuant to section 39(4) of the Act, a public body may use the information only to the extent necessary to carry out its purpose in a reasonable manner. Section 39(4) of the Act states:

39(4) A public body may use personal information only to the extent necessary to enable the public body to carry out its purpose in a reasonable manner.

[para 74] AHRC's submissions state that the Complainant's personal information was used "in a minimal and sensitive manner by a very small number of people under the oversight of JSG lawyers who are bound by strict confidentiality rules" (at page 19).

[para 75] The submissions before me indicate that JSG kept only the information it needed to manage the Complainant's termination, including the related legal proceedings. It states that this information contained only a small amount of personal information.

[para 76] Given the above, I find that JSG did not use the Complainant's personal information beyond what was necessary for its purposes.

4. Did AHRC and/or JSG disclose the Complainant's personal information? If yes, did it have authority to do so under sections 40(1) and 40(4) of the Act?

[para 77] The Notice of Inquiry states:

This includes any disclosure to another public body to review any personal information of the Complainant.

[para 78] The Complainant's complaint, request for inquiry, and submission to the inquiry, are primarily concerned with AHRC retaining the Complainant's files. The only references to an improper disclosure of his information are where the Complainant states that AHRC "released" his information to another government agency (attachment to request for inquiry), and where he states that AHRC improperly allowed "government agencies" to access his personal information (request for inquiry form). In both cases the Complainant seems to be referring to AHRC providing his files to JSG. None of the concerns raised by the Complainant relate to any subsequent disclosure by AHRC or JSG. Therefore, I will address only the question of whether AHRC improperly disclosed the Complainant's personal information to JSG.

[para 79] Section 40(1) of the Act provides authority for public bodies to disclose personal information. I found above that AHRC did not collect the Complainant's personal information, within the terms of the FOIP Act, when the Complainant placed his information on AHRC servers or left tangible records containing his personal information on AHRC premises. I also found that AHRC did not collect his personal information when it gathered up this information and provided it to JSG to sort and return to the Complainant.

[para 80] As AHRC did not collect the Complainant's personal information within the terms of the FOIP Act, it cannot be said to have disclosed that information within the terms of the FOIP Act.

[para 81] While I have found that JSG collected and used the Complainant's personal information, the Complainant did not raise concerns about any disclosures that may have been made by JSG.

5. Did AHRC and/or JSG meet its obligations as required by section 38 of the Act (protection of personal information)?

[para 82] The Notice of Inquiry states

This question is meant to address the Complainant's concern about the absence of a policy for dealing with an employee's personal records on termination.

[para 83] In his request for inquiry the Complainant states that AHRC "has a larger obligation to have a clear policy when they take steps to allow for private spaces to be created and then at the end of employment wanted to breach that privacy by claiming some post-termination protocol."

[para 84] Section 38 of the Act states:

> *38 The head of a public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.*

[para 85] In Order F2018-37, the adjudicator noted that for the obligations in section 38 to arise, the public body must have custody or control of the record. She said (at para. 14):

> While section 38 creates a broad duty to protect personal information, section 4 of the FOIP Act limits the scope of the Act to records in the custody or control of a public body. In other words, if a public body does not have custody or control of records, it has no duty to protect the record under section 38.

[para 86] I found that AHRC did not collect the Complainant's personal information by virtue of his saving information on its servers and/or keeping tangible files on AHRC premises. This principle applies when any employee similarly saves or retains personal files on a public body's premises, computers, or network environment, assuming the public body does not take control of the records for its own purposes, such as managing the employment relationship and/or internal employment investigations (i.e. the conditions set out at paragraph 44 of this Order are met).

[para 87] I agree with the analysis in Order F2018-37. As AHRC did not have custody or control of the Complainant's personal information, it did not have a duty under section 38 with respect to that information.

[para 88] It follows from this that section 38 does not require a public body to have a policy on handling personal information saved or maintained on public body servers or at physical locations by employees, where that personal information is entirely unrelated to the employees' job duties or positions. This is because the FOIP Act would generally not apply where the public body hasn't taken steps to assume control of the personal information.

[para 89] Where a public body collects the personal information for its own purposes, as JSG did in this case, section 38 requires the public body to make reasonable security arrangements to protect that personal information. This requirement does not also include a requirement to have a

policy informing employees of how their personal documents will be handled in the event their employment is terminated (although such a policy might be instructive for employees).

[para 90] I noted that the obligations in section 38 apply such that JSG had an obligation to protect the Complainant's personal information that was retained after his termination. Regarding JSG's duties, AHRC's submission states (at pages 21-22):

> The electronic records are currently stored in secure locations that are accessible by only a limited number of people with JSG's Evidence Production team, the Corporate Information Security Office, and by counsel for the Public Body in this matter and the related proceedings.
>
> Please note: though not the subject of this Inquiry, the Public Body notes that these files (including the electronic files) contained a great deal of personal information of a significant number of individuals other than [the Complainant], and also information that is arguably subject to solicitor and client privilege. The specific steps taken in relation to these files were taken to protect this possible privilege and these individuals' personal information, as well as to protect [the Complainant]'s personal information. These steps were taken for a number of reasons, one of which was to meet the Public Body's duties under FOIP.

[para 91] This satisfies me that JSG took reasonable steps to ensure the security of the Complainant's personal information.

IV. ORDER

[para 92] I make this Order under section 72 of the Act.

[para 93] I find that AHRC did not collect, use or disclose the Complainant's personal information. I find that it also did not have an obligation to make reasonable security arrangements regarding that information.

[para 94] I find that JSG collected the Complainant's personal information that was retained to manage the Complainant's termination. I find that the collection and use was authorized.

[para 95] I find that JSG met its duty to make reasonable security arrangements to protect that information as required by section 38.

_____

Amanda Swanek
Adjudicator