# ALBERTA

# OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

# ORDER F2021-25

June 29, 2021

## ALBERTA JUSTICE AND SOLICITOR GENERAL

Case File Number 006020

**Office URL:** www.oipc.ab.ca

**Summary:** The Complainant complained to the Commissioner and to the Public Body that an employee of Alberta Justice and Solicitor General (the Public Body) had accessed his personal information in databases to which the Public Body has access and then disclosed information about him to an individual, whom he had been dating. Once the individual learned the information, she ended the relationship.

The Adjudicator found that the Public Body had not met its duty to take reasonable security measures to protect against the risk of unauthorized access. She directed the Public Body to comply with this duty in relation to the Complainant's personal information. She recommended that the Public Body create clear policies governing its employees' access to personal information.

**Statutes Cited: AB:** *Freedom of Information and Protection of Privacy Act,* R.S.A. 2000, c. F-25, ss. 38, 72; *Personal Information Protection Act,* S.A. 2003, c. P-6.5, s. 34

**Authorities Cited: AB:** Order P2012-02

## 1. BACKGROUND

[para 1] The Complainant complained to the Commissioner and to the Public Body that an employee of Alberta Justice and Solicitor General had accessed his personal information in databases to which the Public Body has access and then disclosed

information about him to an individual, whom he had been dating. Once the individual learned the information, she ended the relationship.

[para 2] The Commissioner accepted the complaint and referred it to inquiry. The Public Body conducted an investigation into the complaint. It provided the results of the investigation *in camera* during the inquiry.

[para 3] The Notice of Inquiry initially included the questions of whether the Public Body had used and disclosed the Complainant's personal information in contravention of Part 2 of the FOIP Act. The Public Body conceded in the inquiry that an employee of the Public Body had accessed the Complainant's personal information in its databases, contrary to the terms of her employment and its policies. As the Public Body concedes that the information in the databases was accessed by an employee without authority, and there is no evidence to suggest that the Public Body authorized or intended for the employee to access the information, I will consider only the issue of whether the Public Body has made reasonable security arrangements to guard against unauthorized access of this kind.

## II. ISSUE: Did the Public Body meet its duty under section 38 of the Act by making reasonable security arrangements to protect the Complainant's personal information against the risks of unauthorized access and disclosure?

[para 4] Section 38 of the FOIP Act imposes a duty on the head of a public body to make reasonable security arrangements to protect personal information against various risks. It 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 5] In Order P2012-02, the Adjudicator interpreted section 34 of the *Personal Information Protection Act* (PIPA). Section 34 of PIPA is similar to section 38 of the FOIP Act, and states:

> *34 An organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.*

[para 6] The Adjudicator stated:

> To be in compliance with section 34, an organization is required to guard against reasonably foreseeable risks; it must implement deliberate, prudent and functional measures that demonstrate that it considered and mitigated such risks; the nature of the safeguards and measures required to be undertaken will vary according to the sensitivity of the personal information (Order P2006-008 at para. 99).

[para 7] In Order P2012-02, the Adjudicator determined that "sensitivity" refers to the potential consequences if the personal information is disclosed. For example, whether the individual whom the information is about could suffer harm as a result of the disclosure, or could become the victim of identity theft, are relevant questions when determining whether information is sensitive.

[para 8] Like section 34 of PIPA, section 38 of the FOIP Act imposes a duty on a public body to make reasonable security arrangements to protect personal information. In my view, a public body will have met the duty under section 38 if it demonstrates that deliberate, prudent, and functional measures have been adopted to guard against, or mitigate, a foreseeable risk. The extent to which security measures are necessary will depend on the sensitivity of the information, as discussed above.

[para 9] The databases the Public Body maintains, and which were accessed in this case, contain personal information such as contact information and information about charges, convictions, employment, health, and mental health. Personal information of this kind is sensitive and requires more extensive security measures than other kinds of personal information.

[para 10] The evidence before me as to what was accessed, when it was accessed, and who accessed it, is imprecise. The evidence as to the details of the access I have been provided is hearsay, given that the investigation and the interviews to which it refers were prepared for proceedings other than this inquiry. In addition, the various accounts of what transpired and when it transpired are in conflict on material points. However, as the Public Body has conceded that there was unauthorized access of the Complainant's personal information, I do not need to make findings as to what was accessed or disclosed, when it was accessed or disclosed, or by whom. Instead, the focus of this inquiry will be on the adequacy of the Public Body's security measures to prevent this from happening, given the kinds of information located in the databases in which the Complainant's personal information is stored.

[para 11] The Public Body states:

> The employee in her position was assigned access to specific IT Systems, specifically the Official Records and Correctional Administration (ORCA) and Justice Online Information Network (JOIN) programs required to "do her job", however in this situation the access to and disclosure of the Complainant's personal information was not work related.
>
> The actions of the employee were an unauthorized access performed by the employee acting outside her position responsibilities.
>
> The employee in accessing the Complainant's personal information was not authorized by JSG and was contrary to JSG's policies, Code of Conduct and Ethics for the Public Service of Alberta (Code of Conduct). Attached.

[para 12] The Public Body attached copies of its relevant policies and the Code of Conduct and Ethics for the Public Service of Alberta.

[para 13] The Public Body's JOIN Acceptable Use Policy, which establishes rules for accessing the JOIN database, states:

> Unacceptable use of JOIN can bring risk to the correct functioning of JOIN and impacts Albertans who rely on agency use of JOIN to provide services.
>
> Unacceptable use can cause major disruption to JOIN, including loss of valuable data and resources.
>
> Unacceptable use can negatively impact the reputation of the Alberta Courts and the Government of Alberta.
>
> **Users and agencies must not use JOIN for any purpose other than as specifically identified in the user's or agency's Access Agreement. For additional clarity, users and agencies must not use JOIN for:**
>
> 1. Sharing information from JOIN by any means, except to deliver authorized services;
> 2. Engaging in any activity that would circumvent the privacy of personal or confidential information, including client information, trade secrets, proprietary financial information, or similar materials without authorization;
> 3. Any activity that is racist, sexist, pornographic, sexual or erotic, obscene, hate inciting, abusive, or contravenes human rights legislation;
> 4. Engaging in illegal activity to intentionally disable, overload, hack, or crack JOIN resources or systems, whether internal or external;
> 5. Harassing or contacting any person or organization; or
> 6. Any other personal or commercial use.
>
> If users are not sure whether their use of JOIN is safe and acceptable, they are expected to consult with their supervisor or JOIN Access Agreement Holder. The supervisor or the Holder should consult with JOIN Operations when they require confirmation of safe and acceptable use.

Employees who are authorized to access the JOIN database to perform their work duties sign the foregoing policy to acknowledge its terms.

[para 14] The Public Body's policy regarding the ORCA [Offender Records and Correctional Administration] database states:

> All employees and Third Parties are responsible for ensuring reasonable and appropriate usage of ORCA information and the system in accordance with the Freedom of Information and Protection of Privacy Act, and the employees and third parties are expected to use discretion and good judgment when accessing ORCA
> • All Government of Alberta employees are responsible for ensuring reasonable and appropriate usage of ORCA information and the system with the Code of Conduct and Ethics for the Government of Alberta and the Official Oath.
> • Employees and contractors must sign an agreement to comply with the ORCA Security Policy, having read and understood it.
> • Sharing of user-IDs and/or passwords or permitting its use by any other unauthorized person is not permitted. [my emphasis]

> • The deletion, examination, copying or modification of data for which other users are responsible is not permitted without prior consent of the Manager, IT Branch, Corporate Services Division.
> • Users are responsible for following all policies and procedures relating to security and confidentiality. In particular, accessing restricted or sensitive information that is not required in the normal course of duty is not permitted. [my emphasis]
> • Unauthorized decryption of any encrypted information or any attempts to do so, are not permitted.
> • Any Alberta Government employee who intentionally causes loss of ORCA data or damage to the system may be subject to disciplinary action up to and including dismissal.

[para 15] The foregoing policy defines "sensitive" in the following way:

> Sensitive: documents, files or records containing personal or "internal use only" information that should not be released to the general public or to unauthorized personnel. Most information in or relating to ORCA is sensitive. Access to this information will be provided on a "need to know" basis (see following section).

***Analysis***

[para 16] Adopting policies regarding use and disclosure of personal information in databases is a reasonable security measure to protect personal information. However, I believe that the instruction given to employees regarding access to databases could be simplified and clarified in order to achieve greater compliance with the FOIP Act and other rules governing use of the Public Body's systems.

[para 17] When I review the JOIN policy, it is unclear to me that an employee would understand from it that merely *accessing* personal information, for unauthorized purposes, is prohibited. While the policy prohibits "engaging in any activity that would circumvent the privacy of personal or confidential information, including client information, trade secrets, proprietary financial information, or similar materials without authorization", an employee might not understand that this prohibition includes accessing or viewing personal information in a database when the employee does not have an authorized employment purpose to do so. The policy does not explain what "circumvent the privacy" means, or what "authorization" means in the context in which these terms are used. This prohibition could be construed as prohibiting unauthorized access; however, it is not plain and obvious that this is the meaning of the prohibition, given its references to trade secrets and proprietary financial information.

[para 18] The ORCA policy does address access. However, it expressly addresses access to "restricted" or "sensitive" personal information, but not personal information that is neither "restricted" nor "sensitive". "Sensitive" personal information is defined in the policy as information that should not be disseminated to the public and is accessible on a "need to know basis". According to the policy, most information in the ORCA database is sensitive. Given that the policy indicates "most" information in ORCA is sensitive, but does not state that *all* personal information in the database is sensitive, the policy is open to the interpretation that some personal information may be accessed *without* a work-related purpose. However, section 38 of the FOIP Act applies to *all* personal information, although sensitive personal information may require more robust security measures than less sensitive information.

[para 19] It may be difficult for an employee to discern which information is sensitive and which is not, when the employee is authorized to access and use personal information in the database regularly as part of work duties. Some kinds of information may not seem to be sensitive to an employee when the employee is authorized to view it and is used to dealing with it on a regular basis.

[para 20] I note, too, that the ORCA policy only refers to employment consequences in relation to damaging or destroying data in the ORCA database; the policy does not refer to employment consequences for other contraventions of the policy. The Policy also requires the database to be used in accordance with the Code of Conduct. I agree that there may be some overlap between the Code of Conduct and compliance with the FOIP Act; however, the Code of Conduct is primarily concerned with conflict of interest i.e. the situation in which an employee of the public service seeks to benefit from information in the custody or control of the Government of Alberta. There are circumstances in which one could comply with the Code of Conduct, but still access personal information without authority. For this reason, requiring compliance with the Code of Conduct may not promote compliance with section 38 of the FOIP Act.

[para 21] I acknowledge that the policy also requires employees to comply with the FOIP Act: however, the FOIP Act does not expressly impose duties on the *employees of public bodies*, but on *public bodies*. Requiring employees to comply with the FOIP Act without explaining how the employees' actions may contribute to, or undermine, the Public Body's compliance with the terms of the FOIP Act may not be sufficiently clear to deter conduct that could cause the Public Body to contravene the FOIP Act.

[para 22] The Public Body's policy restricts password sharing. This is a sensible and reasonable security measure. However, the policy, as written, is confusing. As noted above, it states: "Sharing of user-IDs and/or passwords or permitting its use by any other *unauthorized* person is not permitted." The addition of the word "unauthorized" creates ambiguity. While I believe the policy means that no one is authorized to access any information from the database using someone else's password, the policy is open to the interpretation that an employee who is *authorized* to access a database could do so if someone else authorized to use the database has used their password to open it. An example would be when an employee has signed onto a database and another authorized employee then uses the computer and accesses personal information in the database to perform work duties. This practice is not clearly banned by the policy. However, when employees perform authorized activities using another employee's password, it can create the appearance that the employee who signed onto the database has accessed personal information without authority. Using someone else's password can also hide the fact that an unauthorized access is being made. Being unable to determine precisely who has accessed information and for what purpose undermines the ability of a public body to enforce its security measures. I make these comments because the Public Body's *in camera* evidence leads me to believe that its investigation may have been hampered by an inability to determine with certainty which employees accessed the Complainant's personal information at particular points in time.

[para 23] Given the issues I have identified, it is unclear to what extent the policy deters accessing personal information in the ORCA database without a valid employment purpose. It is possible that the Public Body provides verbal training to its employees regarding the policies that is more explicit regarding unauthorized access than its formal policies. Regardless, the written policy may create the impression it contains "grey areas," with the result that employees view themselves as having discretion over personal information outside the scope of their employment duties, such as viewing a file "proactively" in case it will be assigned to the employee, or viewing information for personal purposes. Further, the policies regarding password sharing are ambiguous, which may also hamper the Public Body in enforcing its security measures.

[para 24] The Public Body provided me with some information regarding the capabilities of its systems. The Public Body's systems have audit functions, which enable it to investigate security breaches and unauthorized accesses. As noted above, when the user who accesses information in the database is not the same as the user who signed onto the database, the audit capabilities are less effective and the Public Body becomes less able to determine who accessed information and whether the access was with or without authority.

[para 25] Employing an audit function is a reasonable security measure to mitigate the risk of unauthorized access. However, given the sensitivity of the information in the Public Body's databases, the limitations on its audit functions, and the lack of clarity in its policies, section 38 requires that it institute clear policy rules to enable the audit function to guard against unauthorized access effectively.

***Order and Recommendation***

[para 26] As I find that the Public Body has not taken sufficient measures to protect personal information in its custody or control from the risk of unauthorized access, I must direct it to comply with this duty in relation to the Complainant's personal information. The Public Body should take whatever measures it considers appropriate to ensure that the Complainant's personal information is not accessed or disclosed without authority.

[para 27] I recommend that the Public Body develop clear and concise policies prohibiting unauthorized access and disclosure by its employees. These policies need not be lengthy, but should be solely dedicated to promoting the Public Body's compliance with section 38. The Public Body's existing policies appear intended to ensure that the Public Body's employees comply with all policies and legislation that may apply to the use of its systems. However, some of the policies and legislation to which the Public Body's policies refer have purposes other than compliance with section 38 of the FOIP Act, or do not directly apply to employees, with the result that the policies do not clearly prohibit unauthorized access to personal information. It is therefore necessary to provide simple rules to enable the Public Body's employees to understand when access to personal information is authorized. In addition, these policies should set out potential employment consequences for unauthorized access to ensure that the policy is

enforceable. Enacting such policies would strengthen the utility of the Public Body's audit functions.

## III. ORDER

[para 28] I make this Order under section 72 of the Act.

[para 29] I order the Public Body to take reasonable security measures to protect the Complainant's personal information in its databases from the risk of unauthorized access and disclosure.

_____

Teresa Cunningham
Adjudicator
/as