Yukon
Information
and Privacy
Commissioner

211 Hawkins Street, Suite 201
Whitehorse, Yukon Y1A 1X3
T: 867.667.8468
F: 867.667.8469
1-800-661-0408 ext. 8468
www.ombudsman.yk.ca

Access to Information and Protection of Privacy Act

INVESTIGATION REPORT

File ATP16-22I

Parties: **Public Service Commission and the Complainant**

Date: **October 24, 2018**

Provisions: **3, 29(a), 29(c), 30(1)(a)(i), 30(2)(a), 30(2)(b), 30(2)(c), 33, 36(b), 36(c) and 42(b)**

Complaint

[1] On November 3, 2016, a Yukon Government (YG) employee (Complainant), complained that personal information collected about YG employees contained in the PeopleSoft Human Resources Management System (HRMS) was being disclosed by the Public Service Commission (PSC) to other YG public bodies contrary to the requirements of the *Access to Information and Protection of Privacy Act* (ATIPP Act) and that this information was also not properly secured.

Jurisdiction

[2] I have authority under subsection 42(b) to receive complaints from the public concerning the administration of the ATIPP Act, conduct investigations into those complaints and report on those investigations.

Explanatory Notes

[3] All section references in this investigation report (Investigation Report) are to the ATIPP Act unless otherwise stated.

Investigative Process

[4] I assigned the Complaint to two investigators in my Office (Investigators). They subsequently interviewed a number of individuals:[1]

- A/Privacy Officer (PSC);
- Complainant;
- Director, Finance & Administration and A/Director of Policy & Planning (PSC);
- Director, HRMS (PSC); and
- HRMS Analyst (PSC).

[5] They also reviewed the following material:

- 'Benefit Guide: Management, Legal Officers & Deputy Ministers', April 2018;
- Emails and attachments;
- Employee benefits set out in the 'Collective Agreement between the Government of Yukon and the Public Service Alliance of Canada, effective January 1, 2016 to December 31, 2018' and YG Management 'Section M';
- Employee collection and disclosure forms used by PSC, public body human resource branches and the Finance Pay & Benefits Branch;
- 'HRMS Access Request Form (Departmental)';
- 'HRMS Access Request Form (Internal)';
- 'HRMS Access Requests and Info' guide;
- 'HRMS Access Review', March 2015;
- GAM 1.1 'Maintenance of General Administration Manual';
- GAM 3.16 'Employee Documentation, Oaths and Personal information';
- GAM 3.59 'Accommodation for Employees with Disabilities';
- 'Global Notes to Employees';
- PSC Submissions;

[1] The individuals (in alphabetical order) held these positions at the time of the interviews.

- 'Privacy Gaps Assessment Report', May 2015;
- *Public Service Act*, Parts 4 and 12;
- *Public Servants Superannuation Act*, sections 1 and 2;
- 'Security Risk Analyses YG PeopleSoft Report', Yukon Information and Privacy Commissioner, February 2018;
- 'Security Role Review Report', ID YTGSECRCL; run date June 20, 2017;
- 'Setting Up and Administering HCM Security (Chapter 8)', Oracle;
- 'SOP 2 – HRMS Access Request', March 1, 2012 (as updated December 31, 2013);
- 'SOP 58 – Annual Account Audit', September 14, 2016; and
- YG 'Employee and Family Assistance Program'.

Background

YG HRMS

[6] PSC is responsible for the development, maintenance, administration and supervision of the Yukon public service.[2] To facilitate this responsibility, it operates a corporate records system called 'HRMS'.[3]

[7] HRMS, as used by PSC, is based on version 9.2 of Oracle's 'PeopleSoft Human Capital Management' platform, inclusive of four modules (*i.e.* Human Resources version 8.53, Benefits Administration, Payroll for North America and Time & Labor). HRMS utilises a collection of HR functions that enables PSC corporately to increase its productivity, streamline organisational performance and lower its cost of operations. HRMS enables PSC to manage its HR requirements while also focusing on strategic public service initiatives, such as recruiting employees and accurately forecasting future workforce needs.[4]

[2] Section 7 of the *Public Service Act*.

[3] PSC's 'operation' is distinct from the HPW-ICT responsibility to maintain HRMS as an operating system.

[4] HRMS processes such employee personal information as [redacted] bank account details, grievance information, names, dates of birth, addresses, phone numbers, leave information, salary and payroll information, benefits enrolled in, and dependents and their information. The 'HR' module includes demographic data about each employee and, where applicable, their families; emergency contact information; job data; view-only pay cheque access; view-only benefits access; leave reporting; Personal Performance Plans; training and certifications; and grievances and appeals.

[8] PSC collects employee personal information (PI) from the human resource branch of a YG public body (PB-HR)[5] for such purposes as hiring and appeals, benefits, grievances, discipline and so forth.[6] PSC can also modify this PI as needed.[7]

[9] A PB-HR collects PI from employees in its public body to complete their personal and superannuation files. The PB-HR then enters the respective PI into HRMS and modifies it as needed. The PB-HR can update, for example, employee phone numbers, email addresses and emergency contact information.

[10] The Financial Operations Branch of Finance (FIN) collects employee PI from PSC, and indirectly though HRMS, for purpose of payment (*i.e.* salary and wages, bonuses, benefits, withheld taxes). It can update phone numbers, banking information, employee tax data, garnishments and so forth.

[11] The collection of PI occurs at the first point of hire and continues throughout the employee's career up to and including termination or retirement.[8]

HRMS Access

[12] The YG 'Security Role Review Report' shows that PSC and 16 other public bodies have access to HRMS.[9] The Legislative Assembly Office (LAO) also has such access.[10]

[5] A 'PB-HR', for purposes of this Investigation Report, will also include the Women's Directorate and the French Language Services Directorate, notwithstanding that neither directorate, despite their access to HRMS, specifies having a Human Resources officer in their corporate structure.

[6] For purposes of this Investigation Report, the PSC Corporate Human Resources and Diversity Services Branch will not be included in any reference to a PB-HR, notwithstanding their similar roles.

[7] A PB-HR obtains some PI from newly hired employees on behalf of PSC and passes this PI to that public body. As such, PSC will be deemed, for purposes of this Investigation Report, to have 'collected' that PI from the individual.

[8] This Investigation Report will only focus on the electronic PI that is collected, used and disclosed in respect of HRMS, as opposed to PI in other formats such as paper.

[9] Section 3 states that a 'public body' means, amongst other things, *"(a) each department, secretariat or other similar executive agency of [YG]...but for greater certainty does not include [amongst other things]...(c) the Legislative Assembly Office (LAO)..."*

[10] The LAO is not a YG public body for purposes of the ATIPP Act. The question of LAO access to PI contained in HRMS in respect of the complaint is, therefore, not within the ambit of the ATIPP Act to resolve – but it is from the disclosure perspective by PSC. Therefore, for purposes of this Investigation Report, the LAO will be treated hypothetically as if it were a YG public body and counted as such. That brings the public body total to 18.

[redacted]

Other Public Body Employees

[14] [redacted]

HRMS Security

[15] Security arrangements may be implemented in various ways in HRMS, including permission lists and roles, and data permission security (also referred as row security). Permission lists are used to define what a user can and cannot do in a component or page. Permission lists are assigned to roles and roles are assigned, in turn, to user IDs to create user security profiles. Data permission security refers to controlling access to the rows of data in the system.

[16] When a component is opened in HRMS, the system displays a search page. The search page represents the search record and the fields that appear are the search keys and alternate key fields that uniquely identify each row of data. The system uses the information that entered by the user in the key or alternate key fields to select the rows of data that the user wants to view or manipulate. The system adds the user's security profile, including their user ID and the values of the permission lists attached to their user profile, to the database. The 'Structured Query Language' selects a statement, along with the values that the user entered on the search page. The system retrieves the data that matches the criteria from the search page and the user's data permission lists. In addition to the search criteria and the permission lists, the data permission security or row security is also used to determine whether a specific row will be

[11] 'Security Role Review Report' at 7-8.

[12] *Ibid.* at 6.

retrieved for that user. Row security is typically used to limit search results to the rows of data of a specific department, branch, or unit, or to the entire organisation.

[17] There are restrictions in place as to what PI can be viewed by different public bodies. For example, PSC states that FIN has access to payroll information but not to biographical information (*e.g.* [redacted] date-of-birth, grievance records, etc.). A PB-HR has access to biographical PI, but not to payroll PI. This 'column-level' restriction on PI, based on separation of duties, somewhat restricts the access to PI.

[18] PSC, in partial response to a document request on December 15, 2016, provided a 'HRMS Access Request (Departmental)' form. It shows that it is possible to request a specific type of access level for a selected role(s), such as 'My Department Only', 'All YTG', or 'Other (Branch Restricted Access)'. The form also contains signature blocks for the employee, the employee's supervisor, and the public body's [PB-HR] director, the latter of whom approves it. There are no signature blocks for PSC approval.[13]

[19] Recently, PSC adjusted this procedure and stated that it only grants 'YTGFULL' access to PB-HR directors unless a convincing case can be provided to decide otherwise.[14]

[20] In addition to the above form, PSC provided the results of a HRMS 'Security Role Review Report'.[15] It shows that 18 public bodies, including PSC, have the ability to access, add and modify the PI contained in HRMS.[16] In some cases, row security is set to the department code of a user, such as 'DPYTG52' for Environment. In other cases, row security is set more generally to 'DPYTG' or, in the case of PSC and FIN, additionally to 'DPYTGRET'.[17]

---

[13] This indicates that PSC is not the gatekeeper (*i.e.* the final approving authority) when it comes to approving access to HRMS. This level of approval appears instead to have been delegated to other public bodies, more specifically to a PB-HR.

[14] With these measures, PSC is moving in the direction of becoming a gatekeeper for the HRMS system; however, this is not yet formalised nor have any protocols or policies been provided to support the newly intended practices.

[15] Report ID YTGSECRCL, run date June 20, 2017.

[16] See attached Appendix A. It breaks down the number of users. Of the 18 public bodies listed, 17 have access to the full DPYTG database. In addition, eight have access to that part of the DPYTG database restricted to their own public body. Four have access to that part of the DPYTG database restricted to their own public body and another public body. Three have access to that part of the DPYTG database restricted to another public body. Two have access to the full DPYTGRET database.

[17] In short, this report shows the many anomalies arising from the newly adopted rule to grant special privileges only to PB-HR directors. These formerly granted rights are now under review and some changes have occurred. For

[21] PSC also provided the following information.[18]

1. The row security code 'DPYTG' means access level to all YG employees, except retirees.
2. The row security code 'DPYTGRET' means access level to all YG employees and retirees.
3. The last HRMS user access review was conducted in the spring of 2015.

6. A copy of the report used to conduct a HRMS user access review was provided (*i.e.* the HRMS report entitled 'Security Role Review Report', ID YTGSECRL, generated on June 20, 2017).

[22] A short assessment of HRMS security, using publically available information and scenario-based modelling, recently resulted in the detection of a security risk to the overall system.[19]

Representations

[23] PSC made the following representations:

example, when an employee changes position (*e.g.* from a PB-HR director to another function), PSC has adopted a policy to review those particular roles and rights in HRMS as part of that change.

[18] June 20, 2017, email from PSC to investigators @ 1550 hours.

[19] The 'Security Risk Analyses YG PeopleSoft Report', conducted by the Yukon Information and Privacy Commissioner (IPC) in February, 2018, is provided in Appendix B of this Investigation Report. It shows, for example, that where an 'angry employee' or a third party were to attack the HRMS system, their efforts would very likely compromise PI because YG does not follow industry standards for such security and, in addition, has no access control policy for HRMS.

- It relies on two subsections as its legal authority to collect PI. The first is subsection 29(a) and, in support, cites a number of examples:[20]
  - the *Public Service Act* (PSA), Parts 4 and 12; and
  - the *Public Servants Superannuation Act* (PSSA), sections 1 and 2.

- The second is subsection 29(c) and, in support, cites a number of examples:[21]
  - the 'Employee and Family Assistance Program';
  - the 'Accommodation for Employees with Disabilities' program, as per GAM 3.59; and
  - other benefits set out in the collective agreements and Section M.

- When it collects PI directly from an individual under subsection 30(1), it uses standard forms.[22]
  - When it collects PI indirectly about an individual under subparagraph 30(1)(a)(i), it relies on consent forms signed by that individual.
  - When it collects PI indirectly about an individual under paragraph 30(1)(b), it asserts that this is the type of PI that can be disclosed to it by PB-HRs under subsections 36(b) and (c) because the HR management function within government is co-shared with PSC and PB-HRs.

- When it collects PI, whether directly or indirectly, it usually uses forms that contain a 'disclaimer' that meets the notice criteria in subsection 30(2). It also relies on GAM 3.16 'Employee Documentation, Oaths and Personal information'. Further, it provides notice in written correspondence, such as 'Global Notes to Employees'.[23]
- It relies on subsections 36(b) and (c) as its legal authority to disclose PI to employees working in PB-HR and FIN. It states that the disclosure is consistent with the purpose

[20] It also listed the *Territorial Court Judiciary Pension Plan Act* and the *Education Act* but these are not relevant to this Investigation Report.

[21] The first two examples, the 'Employee and Family Assistance Program' and the 'Accommodation for Employees with Disabilities' program, are not part of HRMS; rather, they pertain to a separate case management data system used by PSC's 'Health, Safety & Disability Management Branch'. As such, these examples are outside the scope of this investigation.

[22] PSC provided the Investigators with a number of forms and templates designed to assist employees with 'common HR-related processes and procedures'. They can be found at [redacted], examples of which will be used in evidence for purposes of this Investigation Report.

[23] PSC makes no submission as to other means by which it may provide notice.

for which the PI was collected: human resource management, which includes the administration of employees' pay and benefits under the PSA.

[24] PSC made no representations on section 33.

[25] The Complainant made no representations.

Issues

[26] The issues are as follows:

1. *Does PSC have authority under subsections 36(b) and (c) to disclose PI to employees working in a PB-HR or in FIN?*
2. *Is the PI in HRMS secured in accordance with section 33?*

Analysis

Issue 1: Does PSC have authority under subsections 36(b) and (c) to disclose PI to employees working in a PB-HR or FIN?

[27] To determine if PSC's disclosure was authorised under subsections 36(b) and (c), I must first discern its purpose for collecting the PI and compare the results to the disclosure purpose on which it relies in disclosing the PI to other public bodies. In other words, compliance requires PSC's collection and disclosure purposes to match.

[28] Part of my analysis will also require an examination of how PSC exercises its collection authority.

What is the PI at Issue?

[29] Section 3 defines PI as recorded information about an identifiable individual. It sets out a non-exhaustive list that includes:

a) the individual's name, address, or telephone number...
b) the individual's age, sex, sexual orientation, marital status, or family status,
c) an identifying number, symbol, or other particular assigned to the individual...

[30] Section 3 also defines a 'record' by setting out a non-exhaustive list that includes: *books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means*.

[31] Employees' names, addresses, telephone numbers, identifying numbers (*i.e.* [redacted]), ages, sex, marital status, family status and information about their educational, financial and employment history is the identifiable information at issue. Further, this information exists in an electronically recorded format within HRMS. Such recorded information is, in my view, PI within the meaning of section 3.

What is the purpose of collecting the PI?

[32] The evidence shows that the collection of PI occurs at the first point of hire and continues throughout an employee's career up to and including termination or retirement. PSC relies on subsections 29(a) and (c) for this collection.

Subsection 29(a)

[33] Subsection 29(a) states:

No [PI] may be collected by or for a public body unless

a) the collection of that information is authorized by an Act of Parliament or of the Legislature; ...

[34] PSC submits that it has statutory authority to collect the PI at issue. It cites Parts 4 and 12 of the PSA as such authority but does not refer to specific sections or provide any supporting argument in its favour. It also cites sections 1 and 2 of the PSSA but, similarly, does not include any supporting argument. This makes it very difficult to reach a reasonable conclusion as to whether PSC does have the requisite authority; however, an examination of these Parts is warranted in aid of determining compliance.

[35] Part 4 of the PSA is entitled 'Pay and Allowances'. It consists of 13 sections.[24] In particular, section 68 appears to be germane.

[24] See sections 57-69 of the PSA.

[36] Section 68 states *"An employee is entitled to be paid for their services the remuneration applicable to their position."*

[37] The evidence shows that FIN collects employee PI from PSC, and indirectly though HRMS, for purposes of employee remuneration. This includes salary and wages, bonuses, benefits, and the withholding of taxes. To facilitate this purpose, FIN can update such PI as phone numbers, banking information, employee tax data, garnishments, and so forth.

[38] Given the above, I am satisfied that Part 4 of the PSA gives PSC the authority to collect PI for employee remuneration requirements.

[39] Part 12 of the PSA is entitled 'General'. It consists of 23 sections.[25] In particular, sections 167 and 174 appear germane. For example, section 167 states "Every employee appointed to a position in the public service or employed pursuant to this or any other Act, shall be required to provide to the commission, within three months of the start of their employment, any documents requested by the commission to complete an employee personal file or payroll file or for superannuation purposes." [26]

[40] Put another way, section 167 of the PSA sets out the purpose for which PSC is expressly authorised to collect any information, logically inclusive of PI, that it requires from a newly hired employee. The stated purpose is to enable PSC to complete the personal, payroll and superannuation files of these particular employees.

[41] Section 174 states *"A department of the public service shall maintain any personnel records and statistics that may be required by the commission."*

[42] The evidence shows that PSC, PB-HRs and FIN can modify the PI in HRMS as it pertains to their particular purposes.

[43] Rather than examine each successive section in detail, I am satisfied that the documentary evidence supports PSC's assertion that Part 12 of the PSA gives it the authority to collect PI to complete the above-mentioned files.

---

[25] See sections 167-189 of the PSA.

[26] Section 48 of the federal *Public Service Superannuation Regulations* is authority for collecting PI to establish proof of age in respect of an employee's superannuation file.

[44] In my view, Parts 4 and 12 of the PSA, taken together, meet subsection 29(a). I am also of a similar view that sections 1 and 2 of the PSSA, as they address the superannuation contribution requirements of every public service employee, meet subsection 29(a).

Subsection 29(c)

[45] Subsection 29(c) states:

"No [PI] may be collected by or for a public body unless

c) that information relates to and is necessary for carrying out a program or activity of the public body."

[46] The ATIPP Act does not define 'program' or 'activity'. The Alberta Information and Privacy Commissioner (AB-IPC) considered the meaning of these words in the context of Alberta's *Freedom of Information and Protection of Privacy Act* (FOIPPA) which contains a provision that is identical to subsection 29(c). The issue under examination by the AB-IPC was whether the public body had authority to collect personal information for the purpose of managing its employees under subsection 33(c) of FOIPPA.

[47] In a complaint about an employer surreptitiously installing keystroke logging software in an employee's computer, the AB-IPC considered, amongst other things, if the employer's collection of that information was necessary to manage the people whom it employs to provide its services and, in particular, the specific employee arising from a performance concern.[27] The AB-IPC found that managing employees to provide public services is an essential 'activity' of a public body and that PI collected for the purpose of managing an employee could fall within Alberta's equivalent to subsection 29(c). As such, the provision of public services is the long-term aim, the condition of which is dependent on employee management. Any PI needed to facilitate that management purpose would therefore qualify as an activity of PSC.

[48] For the foregoing reasons, managing employees, in my view, is an activity of PSC for the purposes of subsection 29(c).

[49] However, the collection of PI by a public body to this end must meet a restrictive two-part test. It must 'relate to' a program or activity of the public body and be 'necessary' to their implementation. This recognises the common situation in which a public body is authorised by legislation to administer a program or activity but not to collect PI beyond this specific purpose.

[27] Investigation Order F2005-003 (AB IPC) at paras. 11 and 12.

In this situation, a public body has to decide precisely what PI it needs and then set up a mechanism to collect only that amount.[28]

[50] PSC submits, in particular, that it obtained or compiled PI for the purpose of HR management, including the administration of employees' pay and benefits under the PSA. It does not elaborate further but it does refer to benefits set out in the collective agreements and Section M.

[51] For example, the 'Benefit Guide: Management, Legal Officers & Deputy Ministers' sets out, amongst other things, the 'Dental Plan' available to management employees and legal officers. To access this plan, an eligible individual must 'complete an enrollment form(s) supplied to [them] and forward [the form(s)] to the PSC for processing.[29]

[52] Collection of such PI by PSC would be needed, in its view, to carry out both this program and its related activities, given the focus on employees who can only gain access to the benefits through self-identification and disclosure of their PI.

[53] In applying subsection 29(c), it is an essential activity of PSC to manage employees, the desired outcome of which is to deliver public services. As such, the purpose for collecting the PI by PSC is to compensate and provide benefits to employees so that they can deliver these services on behalf of their public body. The collection, as a key component of that activity, must be on-going because employees progress through their careers and, in the course of this, experience change within their individual circumstances. This necessitates corresponding changes to their personal, payroll and superannuation files.

Relates to...

[28] The AB-IPC has provided a public body with considerable scope in deciding what PI it needs to collect and would only interfere if the decision were patently unreasonable (see Investigation Report 2001-IR-007 (AB IPC) at paras. 26-27). However, in keeping with the ATIPP Act's objective to protect privacy, the amount and type of PI obtained by PSC must be consistent with the common principle of limited collection; that is, just enough to execute the personal, payroll and superannuation files and no more.

[29] [redacted] Article 41 of the 'Collective Agreement between the Government of Yukon and the Public Service Alliance of Canada, effective January 1, 2016 to December 31, 2018' sets out the 'Dental Care Program' available to eligible bargaining unit employees. Like the management/legal dental benefit, enrollment also requires the completion of forms by the employee.

[54] In my view, the collection of PI by PSC throughout an employee's career for personal, payroll and superannuation purposes relates directly to the activity of administering employees so that they can deliver public services through their respective public bodies. As such, I am satisfied that the collection of employee PI to provide compensation and superannuation benefits to that employee is a key component of the administrative activity.

Necessary...

[55] The British Columbia Information and Privacy Commissioner (BC-IPC) looked at the meaning of 'necessary' within a provision similar to subsection 29(c). He found that there is no authority for collecting additional PI in the event that it might prove useful in some, as yet, non-descript way or that it would be merely convenient to have it. He also found that, in assessing whether the collection of PI is necessary, there must be consideration as to the sensitivity of it, the particular purpose for its collection and the amount collected.[30]

[56] The evidence shows that the PI collected by PSC in HRMS enables the provision and maintenance of compensation and superannuation benefits to employees in exchange for the delivery of public services by their respective public bodies. There is nothing to indicate that PSC is not adhering to the limited collection principle as discussed above.

[57] The evidence further shows that the PI collected by PSC consists of, for example, [redacted] bank account details, grievance information, names, dates-of-birth, addresses, phone numbers, leave information, salaries and payroll information, enrolled benefits information and employee dependents' information. Some of this PI could be construed as sensitive, such as PI concerning garnishment or grievances. Some could be considered less sensitive in the context of administering an employee, such as their name and address. However, I am of the view that the PI in this case is highly sensitive because, taken together; it presents a picture of an employee's unique career history and individual circumstances.

[58] Taken together, this PI relates to and is necessary to the activity of administering employees in each public body. As such, I am satisfied that PI collected by PSC in the HRMS for personal, payroll and superannuation purposes meets subsection 29(c).

[59] Having determined that PSC has the necessary authority to collect the PI under subsections 29(a) and (c), I will examine how it exercises this authority. If this is done in accordance with section 30, then it remains to compare the collection purpose with the

[30] F07-10, 2007, CanLII 30395 (BC IPC), at paras. 48-49.

disclosure purpose.

How does PSC collect the PI?

[60] How PI must be collected by a public body is set out by subsection 30(1). It states

A public body must collect [PI] directly from the individual the information is about unless

a) another method of collection is authorized by

i) that individual; ...

iii) an Act of Parliament or of the Legislature;

b) the [PI] may be disclosed to the public body under sections 36 to 39; ...

[61] PSC submits that when it collects PI directly from an individual under subsection 30(1), it uses standard forms. In support, it provides an 80-page attachment of such documents. Part of the attachment is grouped under the general heading 'Yukon Forms and Templates'. An accompanying description states "The forms and templates below will assist you with common HR-related processes and procedures."[31]

[62] The above forms and templates are set out alphabetically. They range, for example, from 'Acting pay request for authorization' to 'WCB – Notification to apply for LTD – Letter for YEU Employees'.[32]

[63] A second part of the attachment has additional forms. They include the '2016 Personal Tax Credits Return', the 'E-Pay Service', and the 'Emergency Contact Information'.

[64] A majority of the forms submitted in evidence by PSC are identified as YG forms.[33]

[65] Except for the forms internal to YG, such as a 'Classification Request' in respect of a job position or a 'Computer Account/Email Application Form', those involving YG-employee

[31] [redacted]

[32] The first four forms, from 'Accommodation Assignment Agreement for Employees Approved for Long Term Disability (LTD)' to 'Accommodation Plan – Return to Work' pertain to the Health, Safety & Disability Management Branch and its case management data system, as separate from HRMS. As such, they are outside the scope of this Investigation Report.

[33] There are three non-YG forms. One is the above-mentioned Canada Revenue Agency tax credit form and two are RCMP forms: 'Consent for the Release of Police Information' and 'Consent for Check for a Sexual Offence for which Record Suspension (Pardon) has Been Granted or Issued (Vulnerable Sector Verification)'. Since these forms are not YG-generated, they are not relevant to this Investigation Report.

interaction, such as an 'Affirmation of Allegiance' or 'Emergency Contact Information' require the employee's signature and a corresponding date.

[66] Given the evidence as submitted, I am satisfied that when PSC collects PI directly from an individual, it uses standard forms.

[67] As stated above, subsection 30(1) has specific exceptions to a public body's direct collection of PI from the individual about whom the PI is about. PSC submits that where it indirectly collects PI under subparagraph 30(1)(a)(i) to administer a program, it relies on certain forms pursuant to that program.

[68] For example, the 'Acting pay request for authorization' form provides for additional remuneration when an employee temporarily takes on an acting assignment at a higher classification level.[34] To receive the stipend, the form requires certain employee PI and the employee's dated signature.

[69] Another example, the 'Compressed Work Schedule Agreement' form provides for an additional 'day off' during a pay period in exchange for the employee working an agreed-on longer set of days in the same period.[35] The agreement requires employee PI and the employee's dated signature.

[70] A third example concerns the 'Overtime Authorization' form. To receive approved overtime in the mode of compensatory time or pay, the form requires employee PI and the employee's dated signature.

[71] Given the evidence as submitted, I am satisfied that these types of forms meet the indirect collection authorized by subparagraph 30(1)(a)(i). Completion of such forms enables PSC to indirectly collect the PI necessary to effect its purpose of HR management, including the administration of employees' pay and benefits under the PSA.

[72] PSC also submits that where it indirectly collects PI under paragraph 30(1)(b), it asserts that this is the type of PI that can be disclosed to it under subsections 36(b) and (c). It provides

[34] [redacted]

[35] [redacted]

no reasoning or evidence in support of its assertion so I am unable to make a determination about whether it has this authority.

Does PSC give any Notice of Collection?

[73] One way to test the veracity of PSC's submission as to the PI collection purpose is to look at the 'notice' obligation placed on a public body in subsection 30(2). It states

> *"A public body must tell an individual from whom it collects [PI] ...*
> *a) the purpose for collecting it;*
> *b) the legal authority for collecting it; and*
> *c) the title, business address, and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection."*[36]

[74] The Oxford online dictionary defines the term 'tell' as "[communicating] information to someone in spoken or written words."[37] As such, paragraph 30(2)(a) requires the public body, on collecting PI from the employee, to let them know why it wants it. One would expect, therefore, that PSC's submissions should align with any notice of purpose provided to the employee verbally or in writing at the point of PI collection.

[75] The forms that PSC has provided in evidence are informative on this matter. None of them are compliant because there is no notice in these forms that meet the requirements of subsection 30(2) in the absence of any concurrent verbal notice at the point of PI collection.

[76] For example, the 'Bank Authorization Form for Direct Deposit', issued by PSC, and sent to FIN on completion, requires the employee to enter their name, in the following manner: "I [enter employee name] hereby authorize the Territorial Treasurer to deposit my cheque…" They are also required to sign and date the form.[38]

[77] Similarly, the employee, at the time of employee documentation (*i.e.* within the first three months of hire), is required to provide their name, [redacted], email, signature and date on an 'E-Pay Service' form so that they can access by email an electronic copy of their

[36] Subsection 30(3) sets out two exceptions to subsection 30(2) but they are not relevant to this Investigation Report.

[37] https://en.oxforddictionaries.com/definition/tell.

[38] See YG(976EQ)F1 Rev.10/2017.

pay advice which, according to the form ”contains all the same information as the paper hard copy of [their] pay advice.”[39]

[78] Another example provided by PSC is the ‘Emergency Contact Information’ form requiring the employee’s name, [redacted], signature and date.[40] It seeks out two contacts for emergency purposes, inclusive of contact name, address, primary/secondary phone numbers and the contacts’ relationships to the employee.

[79] Neither the ‘Bank Authorization Form for Direct Deposit’, ‘E-Pay Service’ nor ‘Emergency Contact Information’ forms contain any language that meets the notice requirements of subsection 30(2).

[80] In addition, despite PSC asserting that it provides notice in written correspondence, such as ‘Global Notes to Employees’, there is no evidence submitted to this effect.

[81] The PSC’s internal website is also problematic as to notice. For example, the ‘HR Practitioner Guide – E-Recruitment System (ATS)’ provides PB-HR personnel with guidance on how to use the ‘E-Recruitment System’ to track and manage the recruitment process. [41] There is nothing, however, within its 156 pages that addresses the purpose for PI collection or the requirement to provide notice as per subsection 30(2).

[82] Another example is the ‘E-Recruitment How-to-Guide’.[42] It is a public five-page document designed to assist external and internal applicants who wish to apply for a YG job posting. As above, there is nothing in the document that addresses the PI collection purpose required by subsection 30(2).

[83] The PSC online document entitled ‘E-Recruitment Onboarding Documents’ sets out a list of forms that PSC intends to be brought to the attention of every newly-hired employees.[43] Of a total of 26 forms, two require ‘E-Signature and completion, five require ‘E-Signature and

[39] This form has no Queen’s Printer identification number. It is simply entitled, ‘E-Pay Service’ and contains at the bottom the following sentence: “If you have any questions or require more information about this service, please contact (name) in Human Resources...”

[40] Like the ‘e-Pay Service’ form, it does not contain a Queen’s Printer identification number. It does, however, contain a sentence just under the heading that states *“Please complete form and return to Human Resources.”*

[41] [redacted]

[42] [redacted]

[43] [redacted]

acknowledgment' and one requires just an 'E-Signature'. Two others require 'Print and notarize', one requires 'Print and completion' and three only require 'Print'. The remainder are 'For Info Only'. However, none of these forms address the PI collection purpose required by subsection 30(2).

[84] These examples notwithstanding, subsection 30(2) does provide for verbal notice. PSC advises that it relies on GAM 3.16 'Employee Documentation, Oaths and Personal information'. Its purpose is to:

> *provide general guidance to employees and departments on the:*
> - *collection, use, retention and disposal of employee's personal information;*
> - *administration of oaths of allegiance and office; and*
> - *documentation of employees.*[44]

[85] GAM 3.16 sets out, in '2.0 Collection/Use of Personal Information', such statements as:

> *2.1 Personal information about employees may be collected by the Employer where the information relates to and is necessary for carrying out a program or activity of the Employer.*
> *2.2 Personal information about an employee must be collected directly from the employee the information is about unless another method of collection is authorized by the employee.*[45]

[86] However, GAM 3.16 does not contain any reference to the written or verbal notice requirement of subsection 30(2). As such, there is nothing to advise PSC, a PB-HR and FIN at the point of direct collection that the collection of PI from an individual about whom the PI is about requires the 'telling' of collection purpose, the legal collection authority and the person to whom collection questions can be directed.

[87] The evidence shows instead that collection of an employee's PI seems to rest on two anecdotal testimonies. The first is an assertion that employees are verbally notified as they concurrently provide their PI on a form. The second is an assertion that the employee does understand, to the fullest extent under the ATIPP Act, why they are providing their PI in response to the instructions given by PSC to fill out whatever forms are at issue. In my view, this points to a failure by PSC to meet the notice requirements of subsection 30(2).

---

[44] [redacted]

[45] *Ibid.* at 3. GAM 3.16 provision 2.1 echoes subsection 29(c). 2.2 echoes subsection 30(1).

Does PSC disclose the PI at Issue to PB-HRs and FIN?

[88] The facts show that for purposes of the ATIPP Act, PSC has control of the PI in HRMS.

[89] PSC allows 18 public bodies to access the PI in these modules at any time.[46] For example, the 'Security Role Review Report' shows multiple entries in which users in any given public body have access, according to their security status, to various PI databases. In my view, 'access' by a public body, other than PSC, constitutes a disclosure under the ATIPP Act by PSC to these public bodies.

[90] The verb 'disclose' is not defined in the ATIPP Act. The Supreme Court of Canada, in *Rizzo & Rizzo Shoes Ltd. (Re)* (Rizzo), is the leading authority for statutory interpretation. It states "There is only one principle or approach, namely, the words of an Act are to be read in their entire context and in their grammatical and ordinary sense harmoniously with the scheme of the Act, the object of the Act, and the intention of Parliament."[47]

[91] Applying Rizzo, 'disclose' is defined in the online Oxford dictionary as "make (secret or new information) known."[48] Put into the context of the ATIPP Act, the term 'disclose' is not ambiguous. To a favourable extent, this dictionary definition can also be informed by the definition of 'disclose' in the *Health Information Privacy and Management Act*. It partially defines 'disclose' "in relation to information in the custody and control of a person, [as meaning] making the information available or releasing it to another person..."[49] As such, I am of the view that 'disclose' in the ATIPP Act can be interpreted as making known or available a record containing PI, in this case, by PSC to another public body, inclusive of making the record accessible by such an entity.

[92] There are 18 public bodies, including PSC, that have user-access to the above PI contained in HRMS. I am satisfied that, at any given time, PSC discloses the PI to all PB-HRs, as well as FIN, through HRMS.

---

[46] *Supra*, note 10. [The LAO is a 'public body' for purposes of this Investigation Report].

[47] https://www.canlii.org/en/ca/scc/doc/1998/1998canlii837/1998canlii837.html?autocompleteStr=RIZZO&autocompletePos=1 at para. 21.

[48] https://en.oxforddictionaries.com/definition/disclose.

[49] S.Y. 2013, c.16, subsection 2(1). The remaining part of the definition, *"but includes neither using the information nor its transmission between a custodian and an agent of that custodian"* is not relevant.

Does PSC have the authority to disclose the PI at Issue to PB-HRs and FIN?

[93] Section 36 is contained in Part 3 and establishes the only circumstances by which a public body is authorised to disclose PI.[50]

[94] PSC submits that it relies on subsections 36(b) and (c) as its legal authorities to disclose PI to PB-HRs and FIN.

Subsection 36(b)

[95] Subsection 36(b) states:

A public body may disclose [PI] only...

b) if the individual the information is about has consented, in the prescribed manner, to its disclosure; ...

[96] The 'prescribed manner' is set out in ATIPP Act O.I.C. 1996/053. Subsection 2(1) states:

An individual's consent under subsection 36(b) of the Act to the public body disclosing [PI] about them must

a) be in writing, and

b) specify to whom the [PI] may be disclosed and how it may be used.

[97] No forms provided by PSC in support of its HRMS submissions, in addition to those available on PSC's internal website, meet the requirement of subsection 36(b). I am of the view, therefore, that PSC cannot rely on subsection 36(b) as a legal authority to disclose PI to employees working in PB-HR and FIN.

Subsection 36(c)

[98] PSC also relies on subsection 36(c). It states:

A public body may disclose [PI] only...

c) for the purpose for which it was obtained or compiled or for a use consistent with that purpose[.]

[50] Part 3 is a complete scheme for governing the collection, retention, security, use and disclosure of PI in the custody or control of a public body.

[99] 'Purpose' is not defined in the ATIPP Act. The Oxford online dictionary is therefore informative. It defines 'purpose' as "the reason for which something is done or created or for which something exists."[51]

[100] PSC's reason for collecting the PI is to manage human resources, inclusive of employee pay and benefits administration under the PSA. The implication, given reference to the PSA, is that this management function is corporate in nature. Based on my earlier-stated view that Parts 4 and 12 of the PSA, as well as sections 1 and 2 of the PSSA, meet subsection 29(a), I am satisfied that the implication is correct.

[101] Subsection 36(c) has two paths. The first authorises disclosure for the purpose for which it was obtained or compiled. The second authorises disclosure for a use that is consistent with that same purpose. They are, however, separate paths. A public body may employ either as sole authority for disclosing PI in its custody or control.

[102] As to the first path, a public body can only disclose PI if there is no incongruity between the purpose for which it was obtained or compiled and the purpose for which it is being disclosed. The purpose must be identical. Anything else would preclude disclosure under this path.

[103] As to the second path, a public body can only disclose PI for a use consistent with the reason for which it was obtained or compiled. The meaning of 'consistent' is set out in section 37.

[104] It states:

> *A use of [PI] is consistent under sections 35 and 36 with the purposes for which the information was obtained or compiled if the use*
>
> *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 the information or to which the information is disclosed.*

[105] If a public body cannot meet this two-part test in section 37, then an inconsistency exists that precludes disclosure. In other words, the reason for obtaining or compiling PI does not align with the reason informing its use.

---

[51] https://en.oxforddictionaries.com/definition/purpose.

[106] PSC relies on both paths of subsection 36(c). It does not differentiate between them so each must be examined as to their applicability to the facts at hand.

Path 1

[107] I have previously determined that PSC is authorised to collect PI from employees so that it can enroll them in YG's pay and benefits system. This is the collection purpose. Since PSC administers this system, it follows that it can disclose this PI to the PB-HR in which the employee works. It can also disclose this PI to FIN so that the employee can be remunerated as to their pay and benefits. Such disclosures align with the original collection purpose. There is no inconsistency between the collection and disclosure purposes.

[108] While it is only necessary for PSC to meet one of the two paths, as it has done, it is nevertheless informative to consider whether it meets the second path.

Path 2

[109] I have previously determined that PSC is authorised to collect PI from employees because such collection informs the activity of administering employees in each public body.

[110] PSC can only disclose that PI if its use is consistent with the purpose for which it was obtained or compiled. PSC submits that it uses this PI to administer each employee's personal, payroll and superannuation files. In my view, this 'use' is reasonably and directly connected to the above purpose. PSC has obtained or compiled the employee's PI so that it can use this PI to recompense the employee in exchange for providing the employer's services. It follows that this 'use' is necessary because the administration of the employee about whom the PI is about enables, in turn, a public body to meet its statutory or programming obligations.

[111] As such, I am of the view that the PI obtained or complied by PSC is consistent with the purpose for obtaining or compiling it: to administer each employee's personal, payroll and superannuation files, thus enabling the delivery of public body services by an employee.

[112] Given the above analyses, I am of the view that PSC's disclosure of the PI at issue to a PB-HR and to FIN is authorised by either path in subsection 36(c). FIN remunerates every employee. This administrative relationship as between these respective entities will require disclosure by PSC to the particular PB-HR and FIN so that the PI at issue can be updated or otherwise modified during the employee's career.

[113] The evidence shows, however, that PSC discloses the PI at issue to every PB-HR simultaneously, as well as to FIN. In other words, all PB-HRs, as well as FIN, have full access to the PI at issue in HRMS.

[114] FIN is responsible for providing a central service to YG because, as stated, it has to remunerate every employee regardless of the public body in which they work. This disclosure of every employee's relevant PI to FIN would be in accordance with a use consistent with the collection purpose because enrolment in the pay and benefits system requires a payment outcome that only FIN can provide. In other words, this central service could not otherwise be provided to meet the corporate-wide remuneration purpose.

[115] The same cannot be said about PSC's disclosure of the PI at issue beyond that of the PB-HR of the particular public body in which the employee works. PB-HRs elsewhere have no function in the collection of PI as it affects employees working in other public bodies. For example, when PSC collects PI about an employee working in Justice, it cannot disclose this PI to Community Services or Education because these public bodies have no responsibility for the Justice employee. There is no consistency of purpose between the PI collected to administer an employee working in Justice and the disclosing of that PI to another public body, other than FIN for the reasons already stated.

[116] Put another way, PSC cannot disclose PI about Justice employees via HRMS to PB-HRs elsewhere without direct consent from the employees concerned, unless these entities provide HR related services to those Justice employees that are consistent with the purpose for which Justice collected the PI. There is no evidence to that effect.

[117] It is also not enough for PSC to put forth, as it has, that widespread disclosure is a corporate necessity in the event of an employee in one public body migrating to another one on a temporary basis. Disclosing PI based on an eventuality that may never occur for most employees is not a disclosure that is authorised by the ATIPP Act.

[118] In sum, I am of the view that PSC's disclosure, through HRMS, of PI about an employee working in a particular public body to the PB-HR of that same public body, as well as to FIN, is in accord with subsection 36(c). However, I am also of the view that PSC's disclosure, through HRMS, of PI about an employee working in a particular public body to all the PB-HRs of different public bodies is <u>not</u> in accord with subsection 36(c) for the reasons stated.

[119] PSC also submits, as per subsection 36(c), that PI can be disclosed to PSC by PB-HRs because the HR management function within government is co-shared with PSC and PB-HRs. I will not address this submission because the issue in this Investigation Report is about PSC disclosing to PB-HRs, not the other way around.

Issue 2: Is the PI in HRMS properly secured in accordance with section 33?

[120] Section 33 states "The public body must protect [PI] by making reasonable security arrangements against such risks as accidental loss or alteration, and unauthorized access, collection, use, disclosure or disposal."

[121] The standard of reasonableness in section 33 is an objective one. In a 2013 report of the BC-IPC entitled 'Investigative Report F13-02', the BC-IPC investigated three breaches of personal health data for research purposes when the BC Ministry of Health failed to translate privacy and security policies into meaningful business practices.[52] In doing so, she looked at section 30 of British Columbia's *Freedom of Information and Protection of Privacy Act* (FIPPA). This section is almost identical to section 33 (of the ATIPP Act).

[122] In her view, the standard of reasonableness does not require perfection but, depending on the circumstances, it may import a high level of rigour. That means the public body must put in place appropriate administrative, physical and technical safeguards to protect PI.[53]

[123] She also stated that the adequacy of these safeguards varies, depending on such factors as

- the sensitivity of the PI;
- the medium and format of the records;
- the estimated costs of security;
- the relationship between the public body and the affected individuals; and
- how valuable the PI might be for someone intending to misuse it.[54]

[124] As the evidence shows, the PI in HRMS that is accessible by all PB-HRs includes biographical information, dependent information, leave information, job position and salary information, and, in the event of a grievance, grievance information. This type of PI is highly

[52] https://www.oipc.bc.ca/investigation-reports/1546. Elizabeth Denham, June 26, 2013.

[53] *Ibid.* at 11.

[54] *Ibid.*

sensitive because it forms a unique picture of the particular individual. It is also well known that the improper disclosure of PI can expose an individual to risk of harm resulting from the improper use of that PI, including identity theft, financial fraud and other legal liabilities.

[125] Such PI requires, therefore, a correspondingly high level of administrative, physical and technical safeguards. Making PI pertinent to only one public body (*i.e.* the one in which the employee works) simultaneously available to all PB-HRs to facilitate, for example, a system-wide practical or functional reality in which employees take on temporary assignments in other public bodies, does not meet that level. This is especially the case where it is unlikely that all PB-HR directors will ever need access to all employees at a given time.

[126] This calls into question the high level of trust that must operate between the public bodies, especially in view of the fact that an individual's PI has a known commodity value on the 'dark web' used by those with criminal intent.[55] As such, the cost to the integrity of one's identity must significantly inform the cost of adequately safeguarding HRMS.

[127] PSC has disclosed, via HRMS, all of this sensitive information to all employees who have been assigned the necessary permission lists and roles to access it. For example, any manager who has such a designation could access the PI of any employee in HRMS outside the scope of that manager's public body despite having no reasonable and direct connection to it, nor any necessity to use it.

[128] At a minimum, the safeguards must incorporate the core access principle of 'need-to-know' or 'least privilege'. In other words, PI access must be limited to authorised persons whose responsibilities require such access, as opposed to their status, rank or office, or on a premise of practical or functional convenience. Moreover, the PI limitation must be informed by the lowest access clearance possible to perform those responsibilities. Given my findings in respect of subsections 36(b) and (c), the safeguards are lacking in respect of the core access principle.

[129] There are also other serious problems with the safeguards. These include the lack of a HRMS access control policy (noting the system performance implications), the lack of (formalised) control by PSC when it comes to approving access to HRMS, the fact that the last HRMS user access review goes back in the spring of 2015, [redacted]

[55] See the 'Security Risk Analyses YG PeopleSoft Report' in Appendix B.

[redacted]

[131] Taken together, this amounts to evidence that PSC has not implemented reasonable security arrangements for HRMS.

[132] Until such major issues [redacted] are mitigated, PSC is not compliant with section 33.[57]

[133] I am of the view, therefore, that PSC does not meet the requirements of section 33 because it has not incorporated reasonable security arrangements in respect of HRMS to protect the PI in question. In short, the security complaint by the Complainant is made out.

Conclusion and Recommendation

Subsections 36(b) and (c)

[134] I have determined that, with the exception of the PB-HR staff in a given employee's public body and the Pay & Benefits staff in FIN, PSC has no authority under subsections 36(b) and (c) to disclose any employee's PI to all YG employees listed, by titles, in Appendix A. As such, PSC is in contravention of the above subsections by virtue of its widespread disclosure of PI practices in HRMS. This amounts to a breach of privacy. I therefore recommend that PSC:[58]

1. immediately revokes access to the PI of all employees in row security code 'DPYTG' by all designated employees within the public bodies listed in Appendix A, except for

[56] [redacted]

[57] See Appendix B 'Security Risk Analyses YG PeopleSoft Report' at 15 for this term. 'Rogue' also applies.

[58] As to the LAO and its similar access to HRMS, my recommendations also apply as if the LAO were a public body.

PSC, and replaces it with access only to the PI of those employees working within that designated employee's public body;

2. revises its corporate 'temporary assignment' process so that when an employee in one public body temporarily moves to another public body, the employee's PI is only shared amongst PSC and the two PB-HRs in the respective public bodies and none other;

3. immediately revokes access to the PI of all employees contained in row security codes 'DPYTG' and 'DPYTGRET' by any designated employees within the public bodies listed in Appendix A who do not have any reasonable and direct connection with these employees and a statutory or operational necessity to provide them with anything;

4. develops and implements, in accordance with standard security practices, an access control policy that, at the very least, communicates YG's intention and direction in respect of access control;

5. provides me with an updated HRMS 'Security Role Review Report' once recommendations 1 and 3 are accepted/implemented; and

6. provides me, within six months of the date of receipt of this Investigation Report, a timeframe for implementing recommendations 1 to 5.

Section 33

[135] I have determined that the PI collected about YG employees that is contained within HRMS is not properly secured in accordance with section 33. I therefore recommend that PSC:[59]

7. mitigates, as quickly as possible, the [redacted] issues stated in this Investigation Report; and

8. provides me, within six months of the date of receipt of this Investigation Report, a timeframe for implementing recommendation 7.

[136] A disclosure without authority under the ATIPP Act constitutes a breach of privacy under section 33. In keeping with my determination that PSC disclosed the PI contained in the HRMS

[59] *Ibid.*.

to public bodies without authority, it must undertake the following actions in respect of this privacy breach:

- contain the breach;
- evaluate the risks;
- determine if notification of affected persons is necessary; and
- develop/implement prevention strategies to reduce the likelihood of future breaches.

[137] To ensure these steps are taken, I recommend that PSC:

9. provides me with a breach report, within six months of the date of receipt of this Investigation Report, detailing the steps it took in respect of the breach of privacy.

[138] Given the degree of risks identified in respect of the PI in HRMS, I further recommend that PSC:

10. engages an expert third party to review its HRMS system (*i.e.* server/software) and infrastructure for compliance with industry standards;

11. works in good faith with my Office on the development of a privacy impact assessment (PIA) and a security threat risk assessment (STRA) of HRMS; and

12. begins the work pertaining to recommendations 10 and 11 within 60 days of the date of receipt of this Investigation Report.

Subsection 30(2)

[139] I determined that PSC is not meeting its notice obligations under subsection 30(2). I therefore recommend that PSC:

13. revises GAM 3.16 to include adequate reference to the written or verbal notice requirement of subsection 30(2), thus making it clear at the point of collection by PSC, PB-HRs and FIN that the collection of PI from an individual about whom the PI is about requires the 'telling' of collection purpose, the legal collection authority and the person to whom collection questions can be directed;[60]

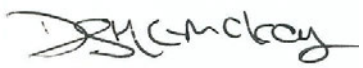
[60] I recognise that the revision process is set out in GAM Policy 1.1 'Maintenance of General Administration Manual'.

14. revises all PI direct collection forms used by PSC, PB-HRs and FIN by incorporating a written 'notice' statement that meets the requirements of subsection 30(2);

15. revises all PI disclosure forms used by PSC, PB-HRs and FIN by incorporating a written statement that meets the 'prescribed manner' consent requirements of subsection 36(b);

16. trains staff on the requirements in GAM 3.16; and

17. provides a copy of the revised documents aforementioned and confirmation that the training has occurred within six months of the date of receipt of this Investigation Report.



_____

Diane McLeod-McKay, B.A., J.D.
Information and Privacy Commissioner

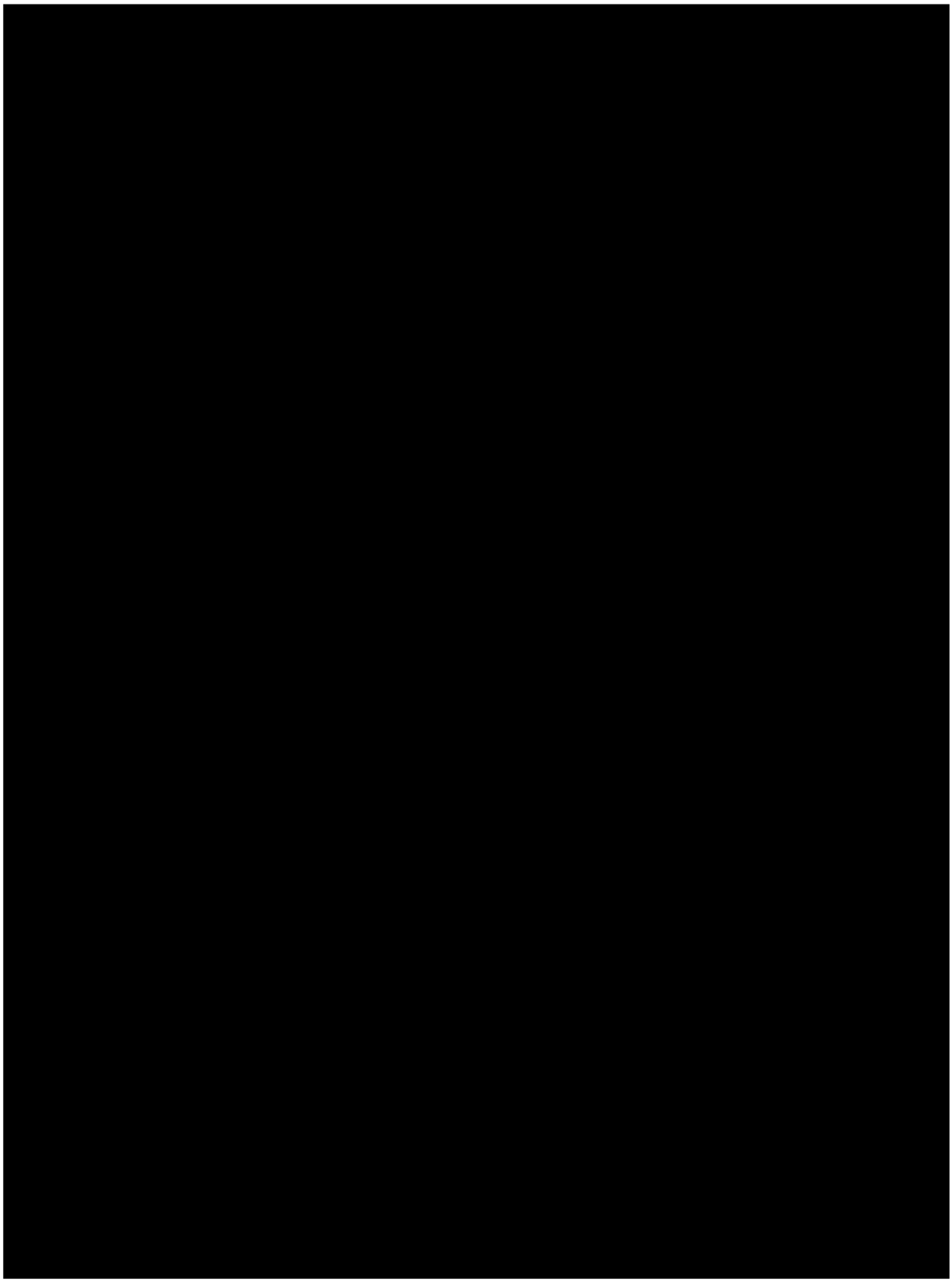
Observation/Appendices

Appendix A

[redacted]

[redacted]

[redacted]



[redacted]

[redacted]

Appendix B

HRMS 'Security Risk Analyses YG PeopleSoft Report'

(See attached IPC document).