Capilano University

Privacy Impact Assessment

ADP Workforce Now

Table of Contents

PART 1: GENERAL INFORMATION

Initiative Title:	ADP Workforce Now

Department:	Finance
PIA Drafter Name:	Jacquetta Goy, Privacy Officer / Max Aryamand Cybersecurity Manager
Initiative Lead Name and Title:	Holly Hunter, Director Financial Operations
Executive Sponsors	

General information about the PIA:

Is this initiative a data-linking program under FIPPA? If this PIA addresses a data-linking program, you must submit this PIA to the Office of the Information and Privacy Commissioner. No
Is this initiative a common or integrated program or activity? Under section FOIPPA 69 (5.4), you must submit this PIA to the Office of the Information and Privacy Commissioner. No
Related PIAs, if any: It has not been possible to verify that a PIA was completed when ADP was initially implemented so this PIA looks at the payroll system from end to end.

1. What is the initiative?

Describe your initiative in enough detail that a reader who knows nothing about your work will understand the purpose of your initiative and who your partners and other stakeholders are. Describe what you're doing, how it works, who is involved, and when or how long your initiative runs.

This initiative is to move the Payroll files for faculty members (and BCCIE which the University manages on their behalf) currently collected and stored through ADP PaySpecialist and hosted in Canada to WorkForce Now which is a cloud-based platform that involves some information being stored on servers in the US. There are no other changes to the Payroll system, and this PIA is limited to the change from PaySpecialist to Worksforce Now.

2. What is the scope of the PIA?

Your initiative might be part of a larger one or might be rolled out in phases. What part of the initiative is covered by this PIA? What is out of scope of this PIA?

This PIA relates to the collection of financial information for the purposes of payroll.

3. What are the data or information elements involved in your initiative?

Please list all the elements of information or data that you might collect, use, store, disclose or access as part of your initiative. If your initiative involves large quantities of information or datasets, you can list categories or other groupings of personal information in a table below or in an appendix.

The following information is currently collected from new starters and entered into PaySpecialist. It is assumed the same set of information will be needed for WorkForce Now but confirmation is being obtained that there are no other data fields and whether gender and marital status will still be required fields.

- Legal Name (required)
- Address (required)
- Date of Birth (required)
- Gender (required)
- Marital Status (required) Note that current practice has been to enter "single" for everyone.
- Status Indian (if aTD1N has been provided by the new starter)
- Social Insurance Number (required)
- Bank Account information for Direct deposit (Bank/ Branch/ Account Number) (required)
- Gross Pay
    - Regular Pay (Sections, Lab, PMI)
    - Other Pay (Spending account, Leave Pay, Multi-location Pay, CSEE, Parental leave top up, etc.)
- Applicable deductions and credits.
    - CPP
    - EI
    - Tax
    - College Pension
    - Life Insurance
    - ADD
    - STD
    - Union Dues

3.1 Did you list personal information in question 3?

Personal information is any recorded information about an identifiable individual, other than business contact information.

Personal information includes information that can be used to identify an individual through association or reference.

Yes

4. How will you reduce the risk of unintentionally collecting personal information?

This question is not relevant for this PIA as personal information is intentionally collected.

PART 2: COLLECTION, USE AND DISCLOSURE

This section will help you identify the legal authority for collecting, using and disclosing personal information, and confirm that all personal information elements are necessary for the purpose of the initiative.

5. Collection, use and disclosure

Use column 2 to identify whether the action in column 1 is a collection, use or disclosure of personal information. Use columns 3 and 4 to identify the legal authority you have for the collection, use or disclosure.

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	**Collection, use or disclosure**	**FOIPPA authority**	**Other legal authority**
Step 1: New starters are sent an email by HR asking them to complete and send to payroll a Direct Deposit form, and the TD1BC and TD1. This information is necessary to enable the new employee to be paid.	Collection	26(c)	Income Tax Act (Canada) Income Tax Act (BC)
Step 2: The forms are received by the payroll team and the information entered into the PaySpecialist/ Workforce Now application.	Collection and Disclosure	26(c)	

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	**Collection, use or disclosure**	**FOIPPA authority**	**Other legal authority**
Step 3: Deduction and credit information is added by the payroll team	Use	26(c)	Income Tax Act (Canada) Income Tax Act (BC) Public Pension Act
Step 4: The forms are stored on in the employees HR folder which is in a limited access area of the J drive. Physical forms provided in the past were stored in employee files in locked filing cabinets in filing rooms with limited access.	Retention	26(c)	
Step 6: Workforce Now application backup to ADP datacentres in the USA more detailed location information requested.	Retention	26(c)	
Step 5: A limited amount of information is shared with the College Pension Plan and may be made available to the CRA on request during an audit.	Disclosure	26(c)	Income Tax Act (Canada) Income Tax Act (BC)
Step 6: Records deleted six years after the year that employees leave the University	Destruction	26(c)	Income Tax Act

6. Collection Notice

If you are collecting personal information directly from an individual the information is about, FOIPPA requires that you provide a collection notice (except in limited circumstances).

Forms TD1 and TD1BC include the following notice:

Personal information (including the SIN) is collected for the purposes of the administration or enforcement of the Income Tax Act and related programs and activities including administering tax, benefits, audit, compliance, and collection. The information collected may be used or disclosed for purposes of other federal acts that provide for the imposition and collection of a tax or duty. It may also be disclosed to other federal, provincial, territorial, or foreign government institutions to the extent authorized by law. Failure to provide this information may result in interest payable, penalties, or other actions. Under the Privacy Act, individuals have a right of protection, access to and correction of their personal information, or to file a complaint with the Privacy Commissioner of Canada regarding the handling of their personal information. Refer to Personal Information Bank CRA PPU 120 on Info Source at canada.ca/cra-info-source

A new collection notice needs to be inserted into the communication to new starters when asking for the forms to be completed and additional personal information to be provided. A more formal standard email, letter or form should be created for this purpose. Draft Notice as below.

Capilano University is authorised to collect personal information necessary for its activities under section 26 of the Freedom of Information and Protection of Privacy Act of British Columbia. The information that you provide will be used on a confidential basis, for the purposes of setting up and executing payroll functions for employees of the University. The information may be shared for the purposes of administering payment processes with:

- *financial institutions for the purposes of making payments to employees;*
- *College Pension for the purposes of making pension contributions;*
- *the Canada Revenue Agency to verify details or provide information in relation to payments made; and*
- *our third party payroll service provider Automatic Data Processing Inc (ADP), to support financial administration and payments made to employees. ADP provides a software as a service application to the University with servers in Georgia, USA.*

Any questions concerning the collection and use of this information should be directed to the Privacy Officer: privacy@capilanou.ca.

Communication will also be sent to existing employees about the system change to include the information above.

PART 3: STORING PERSONAL INFORMATION

If you're storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

7. Is any personal information stored outside of Canada?

Yes. ADP servers for Workforce Now are in Georgia, USA, with backups held in other ADP

8. Does your initiative involve sensitive personal information?

Yes, Payroll records are considered to be sensitive personal information.

9. Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)?

No. 33(2)(f) refers to information that is made available to the public.

10. Where are you storing the personal information involved in your initiative?

ADP Workforce Now is a software as a service application with servers in Georgia, USA and backups in other US locations

Confirm the location of backups data storage.

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section if you are disclosing sensitive personal information to be stored outside of Canada. You may need help from your organization's Privacy Officer.

11. Is the sensitive personal information stored by a service provider?

Yes

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?
Automatic Data Processing Inc	Automatic Data Processing Inc	Atlanta, Georgia, USA *Add location of backups*

12. Provide details on the disclosure, including to whom it is disclosed and where the sensitive personal information is stored.

The information collected and used in the payroll system for faculty members will be recorded and processed in Workforce now, a software as a service application provided by Automatic Data Processing Inc. Servers are based in Geogia, USA. Backups are held in other US data centres managed directly by ADP.

Confirm what agreements or obligations ADP has to disclose information to any third parties (eg IRS) and what process it follows with regard to such disclosures.

13. Does the contract you rely on include privacy-related terms?

Yes, the Terms and Conditions are set out in the Global Master Services Agreement, supported by ADP's Trust package which includes brochures on how the company manages data storage, data privacy, third party risk management and other matters. ADP implements Global Security Organization's (GSO) Third-Party Risk Management assessments and requires that third parties comply with ADP data security and privacy policy requirements, as well as ADP's contractual agreements with its clients. ADP have also provided their ISO27000 certification.

15. What controls are in place to prevent unauthorized access to sensitive personal information?

- **Data Center Physical security**

  ADP security policy requires ADP management to identify those areas requiring a specific level of physical security. Access to those areas is provided only to authorized associates for necessary purposes. ADP secured areas employ various physical security safeguards; Schedule 15 [redacted]. Visitors may only be provided access where authorized and are supervised at all times.

- **Data in Transit**

  By policy, ADP requires that all confidential information in transit over a public network which includes all ADP client information) must be encrypted using industry-accepted encryption techniques and strengths. ADP uses industry-accepted cryptographic methods when encrypting client information through well-known transmission protocols such as [redacted] Schedule 21 [redacted]. ADP employs Schedule 21 [redacted] and for administrative access to client information. [redacted] is mandated for all services.

  Data at rest

ADP encrypts all sensitive data stored in file servers, databases, and storage using the latest encryption technologies, such as S 21 .

User Access control

- Controls are in place to prevent unauthorized access to tenant application, program, or object source code,
- Deprovisioning, revocation, or modification of users (employees, contractors, business partners) who have access to the organization's systems and information assets is done in a timely manner as soon as their employment status changes.

16. Provide details about how you will track access to sensitive personal information.

The vendor provides powerful audit trails and system logging for ADP apps to monitor how specific data was accessed by anyone. The auditing system is designed to track the following information:

- Authorized access
- Privileged operations
- Unauthorized access attempts
- Systems alerts or failures.
- Changes to systems security settings, when the system allows such logging.

These logs are only available to ADP-authorized personnel and are sent in live mode to prevent data from being tampered with before being stored in the secure logging appliances.

Besides the auditing systems, ADP also has implemented a central and read-only logging infrastructure (SIEM) and a log correlation and alerting system (TPSI). Log alerts are monitored and treated in a timely manner by the CIRC.

All of these systems are synchronized using a unique Network Time Protocol (NTP) based clock reference.

Each individual log contains, at minimum:

• Timestamp

• Who (identity of the operator or administrator)

• What (information about the event)

17. Describe the privacy risks for disclosure outside of Canada.

Use the table to indicate the privacy risks, potential impacts, likelihood of occurrence and level of privacy risk. For each privacy risk you identify describe a privacy risk response that is proportionate to the level of risk posed.

This may include reference to the measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) you outlined. Add additional rows if necessary.

Privacy risk	Impact to individuals	Likelihood of unauthorized collection, use, disclosure or storage of the sensitive	Level of privacy risk (low, medium, high, considering the	Risk response (this may include contractual mitigations, technical controls, and/or procedural and policy barriers)	Is there any outstanding risk? If yes, please describe.

		personal information (low, medium, high)	impact and likelihood)		
Unauthorized individuals at Capilano University access the payroll personal information	*Identity theft, possible exposure*	*Low*	*Low*	*Access to both PaySpecialist and the J drive area is limited to payroll team members. Access to Workforce Now will have the same restrictions.* *The payroll team understand their confidentiality and privacy obligations.* *A Privacy and Access to Information elearning course has been developed and will be administered to all employees shortly.*	*No*
Unauthorized individuals at ADP access the payroll personal information	*Identity theft, possible exposure*	*Low*	*Low*	*Controls are outlined in 15 and 16*	*No*
Personal information is compromised during transmission.	*Identity theft, possible exposure*	*Low*	*Low*	*All communications utilize* [redacted] S 21 [redacted] *or higher enforced.* *All data is store encrypted-at-rest*	No

				with [redacted] or greater, including backups.	

Outcome of Part 4

The outcome of Part 4 will be **a risk-based decision made by the head of the public body on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 17. **The public body may document the decision in an appropriate format as determined by the head of the public body or by using this PIA template.**

PART 5: SECURITY OF PERSONAL INFORMATION

In Part 5 you will share information about the privacy aspect of securing personal information. People, organizations, or governments outside of your initiative should not be able to access the personal information you collect, use, store or disclose. You need to make sure that the personal information is safely secured in both physical and technical environments.

18. Does your initiative involve digital tools, databases, or information systems?

Yes. A Vendor Security Assessment Questionnaire has been completed and accompanies this PIA.

Based on the outcome of the vendor security assessment, ADP has implemented security controls to securely collect, transmit and store PII (Personally Identifiable Information) of faculty members in their data centres. Once data is stored in their data centres, they use the most advanced encryption technology to encrypt it and enforce technological and physical security controls to prevent unauthorized access.

18.1 Do you or will you have a security assessment to help you ensure the initiative meets the security requirements of FOIPPA section 30?

Yes. The vendor security assessment was performed to guarantee that the initiative complies with the security standards of FOIPPA section 30. Please see the appendix.

19. What technical and physical security do you have in place to protect personal information?

Technical

1. Access control:

ADP has the following within the access control family:

- Security policies and procedures
- Account management
- Separation of duties
- Least privilege
- Remote access
- Unsuccessful logon attempts
- Session termination
- Supervision and review- Access Control

2. Assessment, Authorization, and Monitoring

- Policy and procedures
- Authorization
- Continues Monitoring
- Penetration testing

3. Audit

- Event logging
- Audit record retention
- Session audit
- Audit log storage capacity

4. Awareness and Training

- Policy and procedures
- Training records

5. Incident Response
   - Policy and procedures
   - Incident handling
   - Incident monitoring
   - Incident reporting
   - Incident response plan

6. Personnel Security
    - Policy and procedure
    - Employee screening
    - Employee termination

7. Risk Assessment
    - Vulnerability monitoring and scanning.
    - Privacy impact assessment
    - Threat hunting

Physical

- [redacted]
- [redacted]
- Schedule 15
- [redacted]
- [redacted]

20. Controlling and tracking access

Please check each strategy that describes how you limit or restrict who can access personal information and how you keep track of who has accessed personal information in the past. Insert your own strategies if needed.

Strategy	Yes/No
ADP only allows employees in certain roles access to information	YES
Employees that need standing or recurring access to personal information must be approved by the executive lead	YES
ADP uses audit logs to see who accesses a file and when	YES
ADP uses the latest encryption technology to encrypt data at rest	YES
All computers and laptops are configured such that there is a lockout screen after a pre-defined amount of time.	YES
ADP uses industry-accepted cryptographic methods when encrypting client information through well-known transmission protocols such as Schedule 15 & 21 [redacted].	YES

Strategy	Yes/No
ADP employs Schedule 15 & 21 and for administrative access to client information. [redacted] is mandated for all services.	YES
ADP-secured areas employ various physical security safeguards; including Schedule 15 [redacted].	YES
ADP conducts an annual assessment of its privacy and security policies.	YES
ADP has both technological and business mechanisms in place to perform secure disposal (e.g., Schedule 15 & 21 [redacted]) of archived and backup data.	YES
Fully redundant network components and stateful firewall devices configured in layers are deployed throughout the hosting infrastructure	YES
Describe any additional controls: N/A	

PART 6: ACCURACY, CORRECTION AND RETENTION

In Part 6 you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

21. How will you make sure that the personal information is accurate and complete?

FOIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete.

The personal information used for payroll management is taken from the Direct Deposit and TD forms provided by the individual. Further information on salary pay and deductions is based on role, workload, various employment regulations and is not individual dependent.

Flag: the exception to this is the gender and marital status fields. Confirmation is required that this information is not collected in Workforce Now as this is personal information that is not needed for the purpose of payroll services.

22. Requests for correction

FOIPPA gives an individual the right to request correction of errors or omissions to their personal information. You must have a process in place to respond to these requests.

22.1 Do you have a process in place to correct personal information?

Yes. The University has a procedure for requests to correct personal information. Requests for correction by employees are processed by Payroll with verification required for any change.

22.2 Sometimes it's not possible to correct the personal information. FOIPPA requires that you make a note on the record about the request for correction if you're not able to correct the record itself. Will you document the request to correct or annotate the record?

Corrections will be made directly into the system.

22.3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FOIPPA requires you to notify the other public body or third party of the request for correction. Will you ensure that you conduct these notifications when necessary?

Yes if the information initially supplied was incorrect this would be communicated to the third party as required.

23. Does your initiative use personal information to make decisions that directly affect an individual?

No, the personal information collected does not affect any payroll related decisions which are based on role and activity (eg how many sessions taught).

PART 7: AGREEMENTS AND INFORMATION BANKS

Please provide information about whether your initiative will involve an information sharing agreement, research agreement or personal information bank.

24. Does your initiative involve an information sharing agreement?

No.
Information might on occasion be requested by the CRA as part of an audit but is not routinely or regularly shared.

25. Will your initiative result in a personal information bank?

Yes, but only for payroll related information. The main PIB for faculty members is held by HR

Describe the type of information in the bank: Payroll information including bank account details, tax and benefits deductions and credits
Name of main organization involved: Capilano University
Any other ministries, agencies, public bodies, or organizations involved: Canada Revenue Agency
Business contact title and phone number for person responsible for managing the PIB: Mirela Pop, Manager, Payroll & Benefits

PART 8: ADDITIONAL RISKS

Part 8 asks that you reflect on the risks to personal information in your initiative and list any risks that have not already been addressed by the questions in the template.

26. Risk response

Describe any additional risks that arise from collecting, using, storing, accessing, or disclosing personal information in your initiative that have not been addressed by the questions on the template.

Refer to #17 of this PIA

PART 9: SIGNATURES

You have completed a PIA. Submit the PIA to your Privacy Officer for review and comment, and then have the PIA signed by those responsible for the initiative.

Privacy Office Comments

While there are some privacy related risks in moving the payroll system from being hosted by the University to a software as a service application in the US these are low level in nature given the information collected and the protections in place. ADP plan to host the University's Workforce Now data in Atlanta, Georgia in the USA. Georgia does not currently have rigorous privacy legislation in place as unfortunately a modernizing Privacy bill did not pass through its legislation into law. However, ADP has signed up to robust data security and privacy models, holding ISO27000 certification and aligning its internal policy requirements to the GDPR.

Outstanding issues.

- ADP to confirm where back up date will be stored, and how they would manage any requests for disclosure of information relating to Capilano University would be managed (eg from the IRS about payments made to joint Canadian-US citizens).
- Provision of an up to date list of data fields to be transitioned from PaySpecialist to Workforce Now and to be collected after transition to confirm that the collection of 'gender' and 'marital status' will cease and this information will not be moved from PaySpecialist to Workforce Now.
- A new privacy notice has been drafted which needs to be added to the initial request to new starters to complete the tax and direct deposit forms. The information in the notice will also need to be shared with current faculty members prior to system change over. A decision is required as to when this communication will be made and whether this will be by way of Frontlines post or another method.

Privacy Office Signatures

This PIA is based on a review of the material provided to the Privacy Office as of the date below.

Role	Name	Signature	Date Signed
Privacy Officer / Privacy Office Representative	Jacquetta Goy, Director Risk Management and Privacy Officer	Jacquetta Goy	10 March 2023

Program Area Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored or disclosed, the program area will engage with their Privacy Office and if necessary, complete a PIA update.

Program Area Comments:

Role	Name	Signature	Date Signed
Initiative Lead	Holly Hunter, Director Financial Operations		
Contact Responsible for Systems Maintenance and/or Security Only required if they have been involved in the PIA	Max Aryamand, Cybersecurity Manager	Max Aryamand	03/09/2023
Executive Sponsor	Tally Bains, Vice President Finance and Administration		
Executive Sponsor	Kartik Bharadwa, Vice President People, Culture and Diversity		

Role	Name	Signature	Date Signed
Head of public body, or designate	Tally Bains, Vice President Finance and Administration		