PRIVACY IMPACT ASSESSMENT (Short-Form)

See Guidance for Completion of Privacy Impact Assessments for detail about each of the below questions.

PART 1: GENERAL INFORMATION

PIA file number:

Initiative title:	Xakia Legal Matter Management
Organization:	University of the Fraser Valley
Business or Academic Unit	Legal Counsel Office
Initiative Lead name and title:	Audrey Ackah
Initiative Lead phone:	
Initiative Lead email:	
Privacy Officer:	Stephen Gaspar
Privacy Officer phone:	Ext. 4654
Privacy Officer email:	Stephen.gaspar@ufv.ca

General information about the PIA:

Is this initiative a data-linking program under FOIPPA? 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:

1. What is the initiative?

The Legal Office is wishing to deploy a cloud-based legal matter management solution, Xakia, that does the following:

- Assist with intake and triage by providing a client portal that can be access by UFV business areas to make requests to the legal office
- To establish a system to assign roles and track tasks that are assigned to legal office staff
- Provide means to track and catalog relevant documents and communications related to a legal file. To accomplish this, Xakia will S. 15(1)(l)
- To provide a means, by way of the client portal to make commonly-used templates and legal resources readily available for use by various UFV business units
- To provide visibility of legal request including associated analytics such as the nature of the request, originating business unit

2. What is the scope of the PIA?

The entire initiative is covered by this PIA

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.

Consider segmenting your response into the different categories of people who you will collect different types of information from (e.g. students, administrators, employees, alumni, etc.).

Please include where the information is coming from (directly from users, pulled from pre-existing UFV databases, etc.)

When a file is opened in Xakia, the following information is collected (if applicable):

1. Status (whether a file is "Not Started" or "in progress")
2. The date the service request was received and any associated deadlines or important dates
3. The identity of the office and/or employee (including relevant contact information) that has made the request
4. The name of the Legal Office staff member that will manage the service request
5. The name of any external lawyer or law firm that will assist with the service request
6. The name of any opposing party or other relevant parties related to the service request or legal matter (i.e. the name of an opposing party on a litigation file or the name of the counter party to a contract under review)
7. Category: classification of the nature of the legal matter (i.e. "contract", "personal injury", "real-estate")
8. The anticipated s. 17 and s. 17 related to an issue or matter.
9. s. 15(1)(l)

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. Note: In some cases (but not always) personal information will appear in element 6 above – to the extent that an opposing or other party related to a matter is an individual.

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

Some initiatives that do not require personal information are at risk of collecting personal information inadvertently, which could result in an information incident.

N/A

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: Personal information may be used to identify an opposing or other party related to a legal matter if such a party is an individual. This personal information may be included when a matter is opened or may be added as it becomes relevant to a matter (i.e. an individual with an interest in the matter is discovered)	Collection, Use	Section 26(c), Section 27 and 27 (3) Section 32(a)	
Step 2: Xakia is a cloud-based solution and file information will be stored in its cloud-based solution.	Disclosure	Section33(2)(d), Section 33(2)(t)	

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).

Personal information will not be collected directly from individuals for this initiative. To the extent personal information will be used to identify an opposing or other party, such personal information will have already been collected by UFV under s. 26(c) of FIPPA or, if collected indirectly, such collection will only be as authorized by section 27 and 27(3).

PART 3: STORING PERSONAL INFORMATION

If UFV is 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?

- No

8. Does your initiative involve sensitive personal information?

- No

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

s. 15(1)(l), s. 21– Canadian data centres (as described in Xakia's HECVAT, terms of service, and Privacy Policy: https://www.xakiatech.com/canadian-privacy-policy). UFV has selected to store any data related to this initiative in Canadian-based data centres.

After you answer this question go to Part 4.

PART 4: SECURITY OF PERSONAL INFORMATION

In Part 4 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.

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

Yes

11. If the answer to question 15 is "yes", has UFV's IT Security Office completed a security assessment

Yes, Xakia has provided a HECVAT (Higher Education Cloud Vendor Assessment Toolkit) which has been reviewed by UFV's IT Security Office and determined to meet all relevant requirements.

12. Has UFV's Privacy Protection Schedule and/or Cloud Security Schedule been attached to the Contract?

Yes

PART 5: ACCURACY, CORRECTION AND RETENTION

In Part 5 you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

13. How will UFV make sure that the personal information is accurate and complete?

In general, personal information collected and used in relation to a legal file will be collected by another office at UFV under the authority of section 26(c) of FIPPA. If they are a student they may update their personal information by contacting UFV's Office of the Registrar or accessing their myUFV account. An employee or faculty member may update their personal information by contacting Human Resources or by means of their myUFV account.

If personal information is collected directly by the legal office under the authority of section 26(c) or indirectly, the legal office will correct any such personal information upon request of the individual or their legal representative.

14. 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.

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

- Yes

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

- No

16. Do you have an information schedule in place related to personal information used to make a decision?

FOIPPA requires that public bodies keep personal information for a minimum of one year after it is used to make a decision.

No

Part 6: ADDITIONAL RISKS

17. Has the vendor expressed, either through contract, communications with you, or their privacy policy, their agreement to notify UFV of a privacy breach?

Yes

18. Risk Response (non-security risks)

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.

If you filled in the risk table at Q.14 for sensitive information stored outside of Canada, only include additional risks here.

Add new rows if necessary.

Possible (non-security) risk	Proportionate response / mitigation strategies
Risk 1: s. 15(1)(l), s. 17 [redacted]	s. 15(1)(l), s. 17 [redacted]

PART 7: 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

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	Electronic signature	Date signed
Privacy Officer / Privacy Office Representative	Stephen Gaspar		March 17, 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	Electronic signature	Date signed
Initiative lead			
Contact Responsible for Systems Maintenance and/or Security Required to confirm a security assessment has been completed satisfactorily			