



Privacy Impact Assessment (PIA) for Modo Co-Operative Carsharing

Agreement – Affiliate Memberships

Before you start	1
PART 1: GENERAL INFORMATION	2
PART 2: COLLECTION, USE, AND DISCLOSURE	5
PART 3: STORING PERSONAL INFORMATION	6
PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA	7
PART 5: SECURITY OF PERSONAL INFORMATION	10
PART 6: ACCURACY, CORRECTION AND RETENTION	11
PART 7: PERSONAL INFORMATION BANKS	12
PART 8: ADDITIONAL RISKS	12
PART 9: SIGNATURES	14

Before you start

- This Privacy Impact Assessment (PIA) form is used by VCC to assess whether a new initiative, or proposed significant change to an existing initiative, meets the privacy protection requirements of the B.C. *Freedom of Information and Protection of Privacy Act*. FIPPA’s protection of privacy requirements. A PIA is a legislative requirement ([FIPPA s. 69\(5.3\)](#)) and mandatory before implementing an initiative.
- You/Your refers to the individual responsible for drafting this PIA, who should be an individual from the relevant department or program area with sufficient knowledge to do so. The PIA must be signed by the role within the program area with the appropriate position to hold accountability for this initiative.

- Please include references to other documents when applicable, but do not insert or embed any documents to/in this assessment form.
- Please review the initial assessment questions and contact the Privacy Office at privacyandfoi@vcc.ca before you begin the form, if you have not already. See more guidance about the PIA process, including the supplementary Guidance Document, on the myVCC [Privacy website](#).

PART 1: GENERAL INFORMATION

PIA file number: #2024-014

Initiative title:	Modo Co-Operative Carsharing Agreement – Affiliate Memberships
VCC Department / Program Area:	Campus Planning and Construction Management
Link to VCC initiative website:	
Link to vendor website:	https://www.modo.coop/
Link to vendor privacy policy:	https://www.modo.coop/privacy-policy
Your name and title:	Mary Corbett, Privacy Coordinator
Your work phone and email:	marcorbett@vcc.ca
Initiative Lead name and title:	Ian Humphreys, VP Administration & International Development
Initiative Lead phone and email:	ihumphreys@vcc.ca

General information about the PIA:

Is this initiative a data-linking program under FIPPA? See the definition in Schedule 1 of FIPPA. If this PIA addresses a data-linking program, the Privacy Officer must submit this PIA to the Office of the Information and Privacy Commissioner.	No
Is this initiative a common or integrated program or activity? See the definition of Schedule 1 of FIPPA. Under section FIPPA 69 (5.4), the Privacy Officer must submit this PIA to the Office of the Information and Privacy Commissioner.	No



<p>Does this initiative involve a regular or systematic exchange of personal information between organizations? If yes, this initiative may require an Information Sharing Agreement.</p>	<p>Yes, but disclosure is not an unreasonable invasion of personal privacy and terms of disclosure are outlined in the contract.</p>
<p>Related PIAs, if any:</p>	

1. What is the initiative?

VCC is entering into a Co-Operative Carsharing Agreement with Modo Co-operative for a partnership membership, and to provide 5 co-operative vehicles (Shared Vehicles) and 5 designated parking spaces/electric charging stations for the Shared Vehicles for their exclusive use and free-of-charge to Modo, in VCC’s east parking lot. These Shared Vehicles are a condition of approving the development of VCC’s new building, the Centre for Clean Energy and Automotive Innovation at the VCC Broadway Campus, as required by the City of Vancouver. Modo will be providing 2 Shared Vehicles as soon as possible and the additional 3 upon completion of VCC’s new building. The Shared Vehicles will be available for us by all members of Modo.

As part of the agreement, Modo is also granting VCC a Modo “partnership membership”, which provides VCC with ^{s. 21(1)} membership shares in Modo for the use of VCC Affiliates (VCC employees). Through these membership shares (called “affiliate memberships” in this PIA), VCC employees who apply to Modo and are approved for membership do not need to pay the membership fees themselves, as long as they remain employees with VCC and the agreement between VCC and Modo exists.

VCC will have ^{s. 21(1)} memberships available with the first 2 Vehicles and another ^{s. 21(1)} available after the completion of the new building.

Affiliate memberships are available to VCC employees on a first-come, first-served basis. Employees will apply and register directly with Modo, on an entirely voluntarily basis. Each individual must meet Modo’s membership requirements in order to be approved to become a member with Modo and Modo will directly collect all required information from the individual according to Modo’s Privacy Policy. The application does not involve VCC.

In the application with Modo, an individual will indicate their affiliation with VCC. Upon receiving the application, Modo will contact VCC’s Liaison Role, as named in the contract, with the individual’s name in order to confirm their employment status with VCC. The “Liaison Role” contact will be ^{s. 15(1)(I)} and any People Services Associate will be able to act as the Liaison Role and confirm

the individual's employment and respond within 24 hours. These roles are authorized to have access to employees' employment status.

Once approved by Modo, the affiliate membership covers the cost of the employee's registration for a Modo membership and allows the employee to use all Modo vehicles. Modo does not provide any other information to VCC about the registered employees other than their name in order to confirm their employment status.

Modo will also provide the Liaison Role with a list of the names of affiliated VCC members on an annual basis so that VCC can confirm which members are still current employees of VCC. Modo will remove any individuals who are no longer affiliated with VCC from the affiliate membership, and the cost of their registration will no longer be covered by the agreement between Modo and VCC. Those affiliate memberships would then become available again for other employees to use.

2. What is the scope of the PIA?

The scope of this PIA only considers the information disclosed between Modo and VCC about employees' eligibility status for the VCC affiliate membership. An employee must apply and register independently with Modo and according to Modo's Privacy Policy and terms, and all information shared with Modo is provided on a voluntary basis by the employee and without any requirement or relationship to VCC. VCC has no access to an employee's membership information.

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

Data elements involved are:

- Employee's name
- Employment history (Confirmation of employee's current employment with VCC)

Modo collects all information directly from employees who choose to apply and register for a Modo membership. Employees register independently and indicate that they are affiliated with VCC during registration.

VCC uses the employee's name and employment history (status of employment/confirmation of current employment), collected through an employee's personnel records. The Liaison Role will receive an applicant's name, or the annual list of names of affiliate members, from Modo **s. 15(1)(l)** **s. 15(1)(l)** and will disclose confirmation of an employee's current employment with VCC.

Modo will use the confirmation of an employee's current employment with VCC to approve their membership, or cancel the membership benefits of individuals no longer affiliated with VCC.

5.1 Did you list personal information in question 3?

Yes – s. 13(1)

s. 13(1)

- If yes, are all of the personal information elements **necessary** for your initiative?
 - Yes – the name is required for identifying the individual, and employment status is required to determine eligibility for the affiliate membership.

3. If you answered “no” to question 3.1: How will VCC reduce the risk of unintentionally collecting personal information?

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.

2. Collection, use, and disclosure flow

Describe the information flow of your initiative in the chart below. The table explains the movement of personal information throughout your initiative (column 1) and identifies each time personal information is collected, used, or disclosed (column 2) and under which corresponding FIPPA authority (column 3).

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	FIPPA authority or other legal authority	Specify any potential risks
Step 1: An employee applies to Modo for an affiliate membership, providing all personal information directly to Modo according to their policies and terms, and indicates in their application that they are affiliated with VCC in order to receive an affiliate membership.	Collection	PIPA	

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	FIPPA authority or other legal authority	Specify any potential risks
Step 2: The Liaison Role discloses whether the named individual is an employee of VCC, when Modo contacts s. 15(1)(l) the Liaison Role with the name of an employee to request confirmation of their affiliation with VCC as indicated on the employee's application.	Disclosure	33(2)(d)	Disclosure of any other information about the employee. VCC may only confirm an employee's current employment with VCC.
Step 3: On an annual basis, Modo provides the VCC Liaison Role with a list of names of individuals with affiliate memberships. The Liaison Role confirms which individuals are currently employed by VCC (disclosure). Modo will remove any individuals who are no longer employed by VCC from the affiliate membership per Modo's agreement with the individual.	Disclosure	33(2)(d)	

3. Collection Notice and Consent

Not applicable to this initiative – Collection of VCC's name and employee status by VCC occurs at the start of employment.

6. 1 Collection Notice

6. 2 Consent

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.

4. Is any personal information stored outside of Canada?

No – any personal information disclosed by VCC in this initiative is already collected through employee intake and maintenance of personnel records, and used for purposes consistent with collection (confirmation of employment). Any information that an employee chooses to disclose to Modo is outside the scope of this PIA and is that employee’s choice to provide to Modo based on their Privacy Policy.

5. If you answered yes to Question 7: Where are you storing the personal information involved in your initiative?
6. Does your initiative involve sensitive personal information that will be stored outside of Canada?
7. If you answered “yes” to Question 9: Is the sensitive personal information being stored outside of Canada only because it is being made available to the public under an enactment that authorizes or requires the information to be made public (FIPPA section 33(2)(f))?

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section only if you answered yes to Question 9: you are disclosing sensitive personal information to be stored outside of Canada. This section will require consultation with a representative from IT Services.

8. Is the sensitive personal information stored by a service provider?
 - If yes, fill in the table below (add more rows if necessary) and then go to question 13
 - If no, go to question 12

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?

9. If you answered “no” to Question 11: Provide details on the disclosure, including to whom it is disclosed and where the sensitive personal information is stored.
10. Does the contract you rely on include privacy-related terms?

- 11. What controls are in place to prevent unauthorized access to sensitive personal information?**
- 12. Provide details about how you and will track access to sensitive personal information.**

Describe how you will know if the sensitive personal information is accessed, including access by service providers (e.g. logging access to data). Consult with IT Services to answer this question.

[Answer]

13. 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 new rows if necessary. See Section 3 of the Guidance Document for examples of privacy risks and risk responses and more guidance for how to complete this table, or see the Guidance on Disclosures Outside of Canada.

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

Outcome of Part 4

The outcome of Part 4 will be a risk-based decision made by the role designated accountable for the initiative on whether to proceed with the initiative, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 16.

Is the outcome to proceed with the initiative? [Answer: Yes or No]

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 and/or your vendor need to make sure that the personal information is safely secured in both physical and technical environments.

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

No.

17.1 If you answered “yes” to Question 17: Do you or will you have a security assessment to ensure the initiative meets the security requirements of FIPPA s. 30?

N/A.

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

Personal information is maintained about employees in employees' files s. 15(1)(l)

s. 15(1)(l)

16. Controlling and tracking access

Strategy
We only allow employees in certain roles access to information: Yes – only the Liaison Role will be receiving the name or list of individuals s. 15(1)(l) s. 15(1)(l) and will confirm current employment status. Only approved People Services Associates will receive, view, and confirm the list of individuals.
Employees that need standing or recurring access to personal information must be approved by their managerial lead: Yes – the Liaison Role is approved to access the information required by this initiative, as the Liaison Role will always be a People Services Associate.
We use audit logs to see who accesses a file and when: Not applicable in this initiative scenario – the Liaison Role has access to an employee’s employment status.
Describe any additional controls:

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.

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

People Services maintains records about whether an employee is currently employed by VCC. The Liaison Role will rely on these updated records to confirm an employee’s employment status and eligibility for the affiliate membership.

18. Requests for correction

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

Yes – if the Liaison Role finds they have provided incorrect information about an individual’s employee status, they will be able to contact the Modo contact in writing to provide this correction, and the affiliate membership list will be reviewed annually when Modo contacts the Liaison Role.

21.2 Sometimes it's not possible to correct the personal information. FIPPA s. 29 requires that you make a note on the record about the request for correction if you are not able to correct the record itself. Will you document the request to correct or annotate the record?

Not applicable – eligibility can be corrected by notifying Modo to remove an individual's affiliation.

21.3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FIPPA s. 29 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?

Not applicable – an employee's employment status with VCC will be recorded by People Services and is not information that an individual can correct.

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

No. VCC provides confirmation of an individual's current employment with VCC; Modo uses that information to determine eligibility according to the terms of the membership agreement between the individual and Modo.

20. If you answered "yes" to Question 22: Do you have a records retention schedule in place related to personal information used to make a decision?

N/A.

PART 7: PERSONAL INFORMATION BANKS

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

No.

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.

22. Risk response

Possible risk	Response / mitigation strategies
Risk 1: Liaison Role discloses information about an employee to Modo that they are not	Notify Privacy Office of potential breach; recover the information from Modo; ensure the Liaison

Possible risk	Response / mitigation strategies
authorized to disclose (information not about their position, function, or remuneration with VCC)	Role is aware of their responsibilities in this role and what information may be disclosed.
Risk 2: VCC incorrectly receives additional personal information about an employee from Modo	Notify Modo and return or destroy any information or records that VCC should not have received.
Risk 3: VCC maintains a list of employees with affiliate memberships.	Destroy records of lists received from Modo. Requests for confirmation are transitory and do not need to be retained beyond confirming an employee's affiliation with VCC.

PART 9: SIGNATURES

You have completed a PIA. Submit the PIA to the Privacy Office 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	Surinder Aulakh	Surinder Aulakh <small>Digitally signed by Surinder Aulakh Date: 2024.09.16 06:26:27 -07'00'</small>	Sept. 16, 2024

Program Area Signatures

The PIA must be signed by a role that is able to hold accountability for a PIA, proportionate to the sensitivity of personal information and/or the risks of the initiative. This signature confirms that this PIA accurately documents data elements and information flow at the time of signing. If there are any changes to the overall initiative, including the way personal information is collected, used, stored, or disclosed, the program area will contact Privacy and, if necessary, complete a PIA update.

Program Area Comments:

Role	Name/Position	Electronic signature	Date signed
Role designated accountable for the initiative	Ian Humphreys		Sept 18, 2024