PIA Guidelines: Online Storefront uStore Administration

Overview

This document provides Privacy Impact Assessment (PIA) guidelines for the administration of uStores, which are individually-run online storefronts connected to the DPP TouchNet marketplace platform. Adherence to these guidelines will help to ensure that operating uStores comply with BC's *Freedom of Information and Protection of Privacy Act* (FIPPA) requirements and UBC's *Policy SC14* and related *Information Security Standards* (ISS).

These guidelines are designed to complement the general uStore Administration Guidelines, which cover best practices surrounding general operation and administration of uStores. This document will list requirements and, where applicable, specify factors related to the data collected for uStore operations that will necessitate a uStore-specific PIA.

For more information on how to submit a PIA request, please refer to Privacy Matters @UBC.

General Data Collection, Notification and Consent Requirements

UBC merchants and entities operating uStores must comply with BC's FIPPA requirements surrounding data collection, notification, and consent.

- A privacy notification must be provided to uStore customers explaining the authority under which personal information (PI) is collected and the purpose for which it will be used. For more information on privacy notifications, please refer to the *Privacy Notification* section below.
- Should the uStore intend to disclose the PI or share it with another individual, UBC department, group, or initiative, or external parties, the customer must be informed of what PI will be shared/disclosed, the purpose for which the PI is being shared, and to whom the PI will be disclosed.
- If the collection of PI or the disclosure/sharing of PI is not essential for or directly related to fulfilling the delivery of services offered by the uStore, the uStore must allow the customer:
    - the option of not providing the information requested,
    - to opt-out (by default) of having their information shared or disclosed to others,
    - to freely exercise these rights and not be penalized or refused service for doing so.
- Collected PI must be retained for at least 1 year.

UBC merchants and entities operating uStores may be required to submit a supplementary PIA request depending on a number of factors, such as the nature of PI collected, how such information is used, shared or disclosed, and where it will be stored. For information about what constitutes PI, refer to the Privacy Fact Sheet.

(Continued)

uStore-Specific PIA Required

A uStore-specific PIA is required if any of the following factors apply:

- Any of the following or similar types of high-risk PI elements are collected or accessed: date of birth, SIN number, government-issued identification, personal health information, biometric data, or gender identity.
- Financial related PI (e.g., bank account or credit card number) will be collected and/or stored outside of the TouchNet platform.
- PI will be collected that is not necessary for the purpose of payment processing or not necessary for delivery of the offered service (e.g., demographic information or PI to be shared with vendors).
- PI will be accessed by, disclosed to, or obtained from another unit within UBC.
- PI will be accessed by, disclosed to, or obtained from a third party external to UBC (other than the TouchNet platform).
- If there are changes in how PI is stored or processed outside of Canada, or if any uStore begins to handle data internationally in a manner not previously assessed, a specific assessment is required to ensure compliance with FIPPA and to adequately manage risks associated with international data transfer and storage.
- PI will be used for marketing or promotional purposes, or disclosed to the general public.

uStore-Specific PIA Not Required

If none of the above factors are applicable, then you are not required to complete a uStore-specific PIA. Generally speaking, if the uStore is collecting PI for the sole purpose of payment processing, and if you are not disclosing the information for any other purpose, the uStore can operate without completing a uStore-specific PIA. However, uStore operators are still required to provide a privacy notification (see below).

Tips and Reminders

To ensure compliance with FIPPA and to optimize operational effectiveness of uStores, administrators are encouraged to adhere to the following principles:

- **Data Minimization**: Collect only the information that is directly related to and necessary for the uStore's operations. Avoid excessive data collection to minimize potential risks, and align with FIPPA's requirements.
- **Secure Payment Processing**: Utilize TouchNet's secure payment capabilities to handle all financial transactions. Ensure that transactions are obtained directly through TouchNet to maintain security and integrity.
- **Control Receipt Distribution:** Provide customers with direct access to their invoice/payment receipts. Avoid unnecessary distribution of additional copies to maintain privacy and reduce the risk of data leaks.
- **Robust Data Handling and Sharing**: Ensure all PI collected is securely stored and shared. Implement strict sharing agreements and confidentiality protocols when interacting with third parties. Follow best practices for information security to prevent unauthorized access or breaches.
- **Proactive Data Management**: Establish procedures that allow customers to easily update or modify their PI stored within the uStore. This ensures data accuracy.
- **Data Anonymization and Aggregation**: Where possible, anonymize or aggregate PI data before releasing it to external third parties. This reduces privacy risks and aligns with best practices for data privacy.
- **Regular Reviews and Updates**: Periodically review these guidelines for updates, changes in legal requirements, or shifts in university policies. Engage with stakeholders to ensure these guidelines address current challenges and best practices.

(Continued)

Privacy Notification

Under FIPPA, uStore operators are required to provide a clear privacy notification whenever PI is collected or used. This notification should inform the customer about the purpose of the collection and the authority under which it is collected. This notification need not require an "I agree" click, but must be visible to ensure the customer is informed. Below is a sample privacy notification:

PRIVACY NOTIFICATION

When you perform a transaction with this uStore, we collect personal information such as your name, contact information and payment information under the authority of Section 26(c) of the British Columbia Freedom of Information and Protection of Privacy Act (FIPPA). This information is shared only with the uStore Operator and UBC's payment processor to complete your transaction. No information will be shared with other parties without your consent. For any concerns or questions regarding the use of your information, please contact [Email].

Contact Us

For questions about the information contained in these guidelines or the PIA process, submit a PIA Inquiry.