

PIA Guidelines: Event Management Platforms

Overview

This document provides Privacy Impact Assessment (PIA) guidelines for the administration and operation of various event management platforms, explaining how to ensure compliance with BC's *Freedom of Information and Protection of Privacy Act* (FIPPA) and UBC's Information Security Standards.

The University of British Columbia recently implemented *TouchNet*, a new gateway to third-party payment processors. As part of this development, UBC has established a list of pre-qualified suppliers capable of providing a *TouchNet Ready* event management platform for enterprise-wide use. The use and administration of these *TouchNet Ready* event management platforms constitute the primary scope for these PIA guidelines.

These *TouchNet Ready* event management platforms leverage existing secure payment capabilities within the Digital Payments Platform (DPP) *TouchNet* system and do not require the collection of personal information (PI) for payment purposes. With the support of the *TouchNet* secure payments process, event management platforms do not need to acquire a separate merchant account.

The following *TouchNet Ready* event management platforms have already undergone the PIA process and are approved for use. Event managers are highly encouraged to leverage these platforms:

- **Fourwaves**
- **vFairs**
- **EventsAir**

A PIA Request must be submitted if the above event management platforms do not meet business needs and a new platform is to be sourced. Additionally, a PIA will be required if administrators plan to collect PI through these platforms for any purpose other than event registration and management. For information about what constitutes PI, refer to the [Privacy Fact Sheet](#). For more details on how to submit a PIA request, visit the [Privacy Matters @UBC](#).

General Data Collection, Notification and Consent Requirements

TouchNet Ready event management platforms must adhere to the following privacy-related requirements:

- **Secure Payment Processing:** The platform should fully leverage *TouchNet's* secure payment processes for transactions with users.
- **Privacy Notification:** A privacy notification must be provided to users, explaining the authority under which PI is collected and the purpose for its use. For more details, refer to the *Privacy Notification* section below.
- **Disclosure and Sharing of PI:** If the platform intends to disclose or share PI with another individual, UBC department, group, initiative, or external parties, users must be informed about:
 - The specific PI that will be shared or disclosed,
 - The purpose of the sharing or disclosure,
 - To whom the PI will be disclosed.
- **Consent and Opt-Out Options:** When collection of PI is not essential for the provision of the platform's services, users must be explicitly informed and granted the following options:
 - The choice not to provide the requested PI,
 - The ability to opt-out, by default, from the sharing or disclosure of their PI,
 - The right to exercise these options without facing penalties or service denial.
- **Data Minimization and Retention:** Collect only the information that is necessary for the intended services. Do not retain information longer than necessary. Align retention practices with applicable UBC retention schedules.
- **Supplementary PIA Requirements:** A supplementary PIA request may be required based on several factors, such as:
 - The nature of PI collected,
 - How the information is used, shared, or disclosed,
 - The location where the information will be stored.

(Continued)

Supplementary PIA Required

A supplementary PIA is required under any of the following circumstances:

- Collection or access to high-risk PI elements such as date of birth, SIN number, government-issued identification, personal health information, biometric data, gender identity, financial information (e.g., bank account or credit card numbers).
- Storage of PI outside of Canada.
- Access to, disclosure of, or obtaining PI from another unit within UBC, requiring an assessment to ensure use is consistent with the purpose for which it was originally collected.
- Access to, disclosure of, or obtaining PI from a third party external to UBC (other than the DPP TouchNet platform) for purposes beyond event registration.
- Use of PI for marketing or promotional purposes, or disclosure to the public.
- Involvement of a third-party external to UBC in the project, who may support the use of the tool (e.g. troubleshooting, data backup).

Supplementary PIA Not Required

A supplementary PIA is not required if none of the above factors apply. Typically, if the tools are used solely for event management support — such as confirming reservations, checking attendance, assigning seats, or accommodating special needs like accessibility or dietary preferences — and no PI is disclosed for unrelated purposes, you may proceed without a supplementary PIA. However, administrators must still provide privacy notifications to event registrants and users.

If any event management platform begins to handle data in a manner not previously assessed, a specific assessment is required to ensure compliance with FIPPA and to adequately manage risks, such as those associated with international data transfer and storage.

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 essential for the platform's functionality. This approach minimizes potential risks and aligns with FIPPA principles.
- **Secure Data Handling and Sharing:** Always securely store all PI. Share it only under strict agreements and confidentiality protocols to prevent unauthorized access or data breaches.
- **Proactive Data Management:** Enable participants to easily revise or update their PI stored within the event management platform to ensure data accuracy.
- **Data Anonymization and Aggregation:** Anonymize or aggregate PI wherever possible before sharing it with external parties, reducing privacy risks in line with data privacy best practices.

(Continued)

Privacy Notification

Under FIPPA, informing individuals about the collection and use of PI is required. This notification should inform the customer about the purpose of the collection and the authority under which it is collected. It is not necessary for individuals to agree actively to this notification by clicking “I agree,” if they have been adequately informed. Below is a sample privacy notification:

PRIVACY NOTIFICATION

When you register for an event, the University of British Columbia (UBC) collects personal information such as your name, contact information, payment details, and any personal dietary or accessibility requirements. UBC collects this information under the authority of section 26(c) of the British Columbia Freedom of Information and Protection of Privacy Act (FIPPA). This information is used solely for processing your registration and managing event logistics. It will be shared with the event organizers and UBC’s payment processor only to complete your event registration request and accommodate your needs during the event. This may result in your personal information being disclosed outside of Canada. UBC will not share your information with any other parties without your consent. If you have questions or concerns about the collection or use of this information, please contact: [Email].

Contact Us

For questions about the information contained in these guidelines or the PIA process, submit a [PIA Inquiry](#).