APPROVED
By Isabel Melendez at 9:46 am, Apr 11, 2025

CAPILANO UNIVERSITY

PRIVACY IMPACT ASSESSMENT (PIA)

Cloudbeds Accommodation Booking Management

A. GENERAL INFORMATION			
PIA File Number:	PIA-25-03		
Department/Faculty:	Squamish Student Housing		
Office/School:	Student Success		
Project Manager / PIA Drafter:	John Umunna	**Title:**	Director, Student Housing
Email:	johnumunna@capilanou.ca	**Phone:**	
Privacy Officer:	Isabel Melendez		
Email:	isabelmelendez@capilanou.ca	**Phone:**	
Related PIAs, if any:	None		

1. Description of the Initiative:
To the best of your ability, please provide a detailed description of the initiative, its main objectives, the context in which it functions, the business need for it, and how the objective will meet that need.

This software will be used to manage room bookings for a pilot of summer conference services in student housing at the Squamish campus. The software will allow bookings, room inventory management, payments maintenance and strategic planning for availability.

An assessment of a number of room booking systems was completed prior to purchase. The University of Toronto currently uses Cloudbeds as their online booking system and has been very happy with them.

2. Scope of this 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? Describe what parts of the initiative you are assessing. If a project will be implemented in phases, be sure to explain which phase is being documented in the PIA. Subsequent updates or amendments can be made for other phases as they are developed

The scope of this PIA is limited to the Cloudbeds Software for the summer accommodation project.

PIA approved provisionally for purchase on 28-Mar-2025, with a second review on the 9th April 2025..

3. Elements of Personal Information:

To the best of your ability, please list all the data or information that will be collected, used, processed, stored, disclosed, or accessed as part of the initiative (not just the personal information). This will allow the Privacy Officer to assess all the information involved against what FIPPA considers to be personal information. For example, if conducting a survey, list the different elements of the information being collected as well as a summary of the other types of questions.

As part of this initiative, we will collect, use, process, store, disclose, or access the following types of information:

1. **Personal Identifiable Information (PII):**
    a. Full Name
    b. Home Address
    c. Personal Phone Number
    d. Personal Email Address
2. **Financial Information:**
    a. Credit Card Information (for processing payments)
3. **Other Potentially Collected Data (if relevant to the initiative):**
    a. Transaction History (if purchases such as parking, snacks at check in, laundry soap etc.)
    b. Communication Preferences (if users opt into receiving updates or marketing materials)

This list ensures that the Privacy Officer can assess all collected information against what FIPPA defines as personal information. If additional categories of data are collected, such as demographic information, employment details, or digital identifiers (e.g., IP addresses, cookies), those should also be disclosed as part of this assessment.

4. Sensitive Personal Information:		
	YES	NO
Will sensitive personal information be collected, stored, used, or disclosed as part of this initiative?	☒	☐
Will the sensitive personal information be stored outside of Canada? If so, please fill out Section E.	☒	☐

Sensitive personal information is not defined in FIPPA. Some types of personal information can be considered sensitive because there is a higher risk of harm to individuals if the information is improperly collected, used, or disclosed. Personal information may be considered sensitive depending on the type of information and the context in which it is collected, used, disclosed, or stored.

Examples of sensitive personal information may include:

- *Personal health information*
- *Genetic and biometric data*
- *Personal financial information*
- *Geolocation data*
- *Criminal records*
- *Counselling records*
- *HR records*
- *Payroll records*

As part of this initiative, we will collect, use, process, and store sensitive personal information, including:

1. Personal Financial Information:
    a. Credit card details for payment processing (if applicable).
    b. Transaction history related to purchases or contributions.
    c. Billing address (if collected for payment verification).
2. Personal Address Information:
    a. Home address for communication, registration, or billing purposes.
    b. Mailing address (if different from home address) for correspondence, official documentation, or physical deliveries.

Data is stored in AWS's US-West-2 Region (Portland Metropolitan area in Oregon) but follows applicable local privacy and compliance regulations. Appropriate security measures, such as encryption and restricted access, will be implemented to protect the confidentiality and integrity of this data.

B. COLLECTION & USE OF PERSONAL INFORMATION

1. Description (either a narrative or flow chart) of the linkages and flows of personal information collected, used, and/or disclosed:

Provide a step-by-step description from beginning to end showing how personal information is collected, circulated, processed, stored, and used, as part of this initiative, and if it is disclosed to any third parties. Please include all formats (paper and electronic) from creation or collection until final disposition. This can be demonstrated either via a flow chart, or a numbered list.

Step 1: Collection of Personal Information

- CapU's Newly Created Website Inquiry Form:
  - Users submit inquiries for room and venue rentals through the website, which links to Cloudbeds online booking site.
  - Information collected at this stage includes:
- Collected information may include:
  - Name
  - Home address
  - Personal phone number
  - Personal email address
  - Payment details (credit card information)
  - Booking details (check-in/check-out dates, room preferences)
  - Room allocation
- Manual Entry by Staff (Primarily for Group/Conference Bookings):
  - Some inquiries, particularly for conference and group bookings, may come through direct calls or staff contacts.
  - In these cases, CapU staff will manually enter details into Cloudbeds.
  - Additional details collected may include:
    - Organization/affiliation (if applicable)
    - Billing contact information
    - Estimated number of attendees
    - Parking requirements
  - Group bookings may choose to have an invoice sent if they are university related group bookings

Step 2: Processing & Use

- Cloudbeds system processes the data for:
  - Confirming reservations
  - Processing payments securely
  - Managing guest profiles and preferences
  - Generating invoices/receipts
  - Sending booking confirmations, updates, and promotional communications (if consented)
- The system automatically encrypts and secures financial data to comply with PCI DSS (Payment Card Industry Data Security Standard).

Step 3: Storage

- Personal information is stored electronically within Cloudbeds' secure servers.
- Information may be temporarily cached on local devices (e.g., workstations at reception) but is not permanently stored outside Cloudbeds' servers.

- Paper-based records (if used) are securely stored and later digitized or destroyed per retention policies.

Step 4: Access & Restrictions

- Only authorized personnel (e.g., reservations team, finance team) can access the data via role-based permissions.
- All access is logged and monitored for security purposes.

Step 5: Disclosure to Third Parties (if applicable)

- Payment Processors: Credit card information is securely transmitted to third-party payment gateways (e.g., Stripe, PayPal) for processing.
- Regulatory Authorities (if required): In cases of compliance requests, data may be disclosed following legal obligations (e.g., audit, tax compliance, law enforcement).
- Marketing & CRM Tools (if opted in by the user): Guest preferences and booking details may be shared with integrated CRM/email marketing platforms to send offers and promotions.

Step 6: Retention & Final Disposition

- Personal data is retained based on regulatory compliance and internal policies:
  - Guest profiles: Retained for future bookings, unless a deletion request is made.
  - Financial records: Retained for a legally required period (e.g., tax purposes).
  - Cloudbeds data is stored in Amazon AWS servers using an RDS database. This is stored in AWS's US-West-2 Region but follows applicable local privacy and compliance regulations.
  - Paper-based records (if applicable): Shredded after digitization or stored securely per policy.
- Users can request data deletion in accordance with data protection laws.

Additional Considerations

- Data Security Measures:
  - Encryption of sensitive data in transit and at rest.
  - Regular security audits and compliance with privacy regulations.
  - Access control mechanisms to limit exposure.
- Compliance with FIPPA:
  - Data is stored in AWS's US-West-2 Region (not Canada) but follows applicable local privacy and compliance regulations.
  - No unauthorized international transfers without explicit approval.

PERSONAL INFORMATION FLOW TABLE:

	Description/Purpose	**Type** *(Collection, Use, Retention or Disclosure)*	**FIPPA Authority**
1.	Collection of Personal Information	Collection	Section 26

2.	Processing & Use	Use	Section 32
3.	Storage	Retention	Section 31
4.	Access & Restrictions	Use	Section 32
5.	Disclosure to Third Parties	Disclosure	Section 33
6.	Retention & Final Disposition	Retention	Section 31
7.			

2. Collection Notification:
Will you be collecting personal information directly from the individual the information is about?
If so, please see below the sample of the collection notice you're required to provide.
Please indicate the location and placement of the notice (e.g., a form).

Example of collection notice:
"Your personal information is collected under the authority of section 26(c) of the Freedom of Information and Protection of Privacy Act (FIPPA), as the information relates directly to and is necessary for an operating program or activity of the University. Questions about the collection of this information may be directed to the Privacy Officer at privacy@capilanou.ca".

We are committed to protecting your privacy and personal information through responsible information management practices. We collect, use, retain, disclose and dispose of personal information in accordance with the Freedom of Information and Protection of Privacy Act (FIPPA), other applicable legislation and Capilano University privacy management practices.

This form collects personal information for the purpose of verification of your room booking request. It is collected by Capilano University under (s)(26)(c) of FIPPA. By submitting this form, you are providing your consent for Capilano University to collect and use this information for this purpose. If you have any questions, please contact stay@capilanou.ca..

3. Direct / Indirect Collection (Section 27(1)):
If, for the purposes of the initiative, the personal information will only be collected directly from the individual the information is about, please identify when and where that collection will take place. If the initiative will collect personal information indirectly, (e.g., website cookies, public database) please provide details.

Personal information will be collected directly from individuals in the following instances:

1. CapU Booking Inquiry Website
    a. Individuals submit inquiries via the online form, providing details such as:
        i. Name
        ii. Contact information (email, phone number)
        iii. Requested dates and venue details

    b. This occurs when an individual actively submits a request for room or venue bookings.
2. Cloudbeds Online Booking Page
    a. When an individual confirms a booking, they will enter additional details, including:
        i. Address (if required for invoicing)
        ii. Payment details (processed securely through third-party payment processors)
3. Manual Entry by CapU Staff (For Group & Conference Bookings)
    a. Some bookings, especially for conference and group reservations, may come through phone or email inquiries.
    b. In these cases, CapU staff will enter the details manually into Cloudbeds.
    c. The individual will be informed that their personal information is being collected and processed for booking purposes.

Indirect Collection (If Applicable)

While most personal information is collected directly, some indirect collection may occur:

- Website Cookies (CapU & Cloudbeds Platforms)
    - If the CapU booking inquiry website or Cloudbeds booking page uses cookies, some non-personal data (e.g., IP address, browser type, session data) may be collected to enhance user experience.
    - Any cookie-based tracking will follow the Cloudbeds Cookie Policy and CapU's privacy guidelines.
    - Users will be informed via a cookie banner where applicable.
- Payment Processing via Third Parties
    - While CapU does not store credit card details, Cloudbeds transmits this information to a secure, third-party PCI DSS-compliant payment processor (e.g., Stripe, PayPal).
    - The payment provider processes and verifies transaction details indirectly.

4. Authorization for Collection (Section 26):
Please describe why it is necessary to collect personal information, in order to fulfill the identified purpose(s) of the initiative. The collection of personal information should be limited only to those information items that are strictly necessary.

Authorization for Collection (Section 26 - FIPPA Compliance)

Purpose of Collection:
The collection of personal information is necessary to effectively manage bookings, process payments, and facilitate communication as part of the initiative using the Cloudbeds system. The information collected ensures the efficient operation of accommodation services and guest management while complying with relevant legal, financial, and operational requirements.

Necessity of Personal Information Collection:

The personal information collected is strictly limited to what is necessary for the following functions:

1. Reservation & Guest Management
    a. Full name: Required to identify the guest and confirm bookings.
    b. Contact information (email & phone number): Necessary for sending booking confirmations, updates, and emergency communications.
    c. Home address: Required for billing purposes and record-keeping in compliance with financial regulations.
2. Payment Processing & Financial Transactions
    a. Credit card information: Essential for processing payments securely and preventing fraudulent transactions.
    b. Billing address: Required for payment verification and compliance with financial regulations.
3. Check-in and Guest Verification
    a. Identification details (if applicable, such as passport or driver's license for verification): Required to ensure the guest's identity matches the booking and complies with security or legal requirements.
4. Regulatory and Compliance Obligations
    a. Certain information may be required for legal, tax, or regulatory purposes (e.g., record-keeping for audits or reporting obligations).
5. Operational and Customer Support Services
    a. Personal information allows for efficient customer service, dispute resolution, and communication regarding changes to bookings or policies.

Limiting Collection to Necessary Items

Only the essential personal information required to fulfill these objectives is collected. No additional sensitive data (such as medical records, biometric data, or unnecessary personal details) is gathered beyond what is needed to operate the initiative effectively.

5. Authorization for Use (Section 32):
List the uses of personal information:

See above answer (question 4)

Please respond to the following statements:	YES	NO
Will the information be used only for the purpose(s) for which it was obtained?	☒	☐
To prevent the use of collected personal information for secondary purposes, safeguards are /will be in place on access to both electronic and hard copies?	☒	☐
Will data be anonymized or aggregated at any point for planning or reporting purposes?	☒	☐

How Data Will Be Anonymized & Aggregated

1. Operational & Usage Reports
    a. Data on room and venue bookings may be aggregated to track:
        i. Total number of reservations
        ii. Occupancy rates and usage trends
        iii. Peak booking periods
        iv. Most frequently used spaces
    b. No personally identifiable information (PII) is included in these reports.
2. Financial & Revenue Tracking
    a. Revenue data is aggregated for internal financial planning.
    b. Reports may include:
        i. Total revenue from bookings
        ii. Payment trends (e.g., method of payment usage)
        iii. Invoice and billing summaries
    c. Individual payment details (e.g., credit card numbers) are never included.
3. User Demographics & Marketing Analysis (If Consent is Given)
    a. General demographic insights (e.g., organization type for conference bookings, country of origin) may be analyzed.
    b. This analysis is conducted at an aggregated level, with no personal identifiers attached.
4. Cloudbeds System Reports & Analytics
    a. Cloudbeds provides built-in reporting tools that allow for aggregated insights on:
        i. Booking trends
        ii. Revenue metrics
        iii. Cancellation rates
        iv. Guest preferences (if opted in)
    b. These reports do not contain personal identifiers and are used strictly for operational decision-making.

Safeguards to Protect Personal Data

- No identifiable personal data will be included in planning or reporting.
- Any reports generated will only use aggregated statistics to prevent the possibility of identifying individuals.
- If data is anonymized, it will be processed in a way that ensures it cannot be re-identified.
- Access to reports is restricted to authorized personnel only.

6. Marketing Uses:

Please identify any anticipated uses of personal information for marketing purposes. All marketing via commercial electronic message (email, text message, etc.) must comply with the rules of Canada's Anti-Spam Law (CASL). All marketing via telephone must comply with the National Do Not Call List (DNCL) Rules.

Anticipated Uses of Personal Information for Marketing

- Email Marketing (CASL Compliance Required)
  - If a guest or client opts in, their name and email address may be used for:
    - Promotional offers on future bookings
    - Updates on available venues, conference spaces, or special rates
    - Event or program announcements related to CapU
- Phone-Based Outreach (DNCL Compliance Required)
  - If an individual provides consent, CapU may follow up via phone with:
    - Special event invitations
    - Personalized offers based on past bookings

Marketing Compliance & Safeguards

- All marketing emails and texts will include:
  - An opt-in requirement before any marketing communications are sent.
  - An easy opt-out/unsubscribe option to comply with Canada's Anti-Spam Law (CASL).
- Marketing calls will follow the National Do Not Call List (DNCL) Rules, ensuring that individuals who have opted out do not receive phone-based marketing.
- No personal information will be shared with third-party marketers or external advertisers.
- Marketing will only target individuals who have explicitly consented, and all outreach will comply with CASL and DNCL regulations.

C. ACCESS, DISCLOSURE & STORAGE OF PERSONAL INFORMATION

1. Access to Personal Information:

Identify who will have access to personal information as a result of this project (e.g., teams, roles, or individuals, including any third party service providers, contractors, etc.), what type of personal information will they be privy to, the purposes for which they will have access, and how information will be made available to them/user access assigned?

Who?	Type of PI?	Purpose(s)?	How?
Manager - Student Housing, Squamish	**Full access: Name, phone number, email, tokenized credit card information, address**	**This information is necessary to manage bookings and communicate with guests who have booked accommodations.**	**Web-based application**
	Full access: Name, phone number, email,	**This information is necessary as the**	**Web-based application**

Director, Student Housing and Food Services	**credit card information, address**	**director will handle the above manager's job duties until a manager is hired into the position. After this, the director will need access to the Cloudbeds system to adequately train the new manager or assist duties if the manager is away.**	
Manager, Community Engagement and Events	**Full access for back-end setup**	**Will be setting up the back end of the Cloudbeds booking system and working with the new manager for conference bookings.**	**Web-based application**
Housing Staff	**Names, room numbers, check-in/checkout dates, basic contact information**	**Need information regarding reservations to assist guests, prepare rooms for accommodations, etc.**	**Web-based application**

Provide details about how you will track and monitor access to personal information (e.g., audit trails or physical sign-in and sign-out of files)?
The Cloudbed system has audit trails.
Is there a defined approval process in place for granting access? Is there a person (title) who will authorize and/or revoke access? How/how often will the approval authorities be reviewed to ensure they are current?
The Manager, Student Housing Services, Squamish will be responsible for granting access to employees who need access.
Identify who (title) has the authority to add, change or delete personal information. Is this power limited to a specific individual(s) or anyone with access can add, change, or delete personal information?
The Manager, Student Housing Services, Squamish will be responsible for granting/removing access to employees who need access.
What controls are in place to prevent unauthorized access to personal information (e.g., locked cabinets, key cards, passwords)?
Cloudbeds and CapU have multiple security measures in place to protect personal information from unauthorized access. **1. Electronic Data Security (Cloudbeds & CapU Systems)** • Role-Based Access Control (RBAC):

    - Only authorized personnel (e.g., reservations team, finance staff) have access to personal information.
    - Users are granted the minimum level of access required for their role.
- Password Protection & Multi-Factor Authentication (MFA):
    - Staff accessing Cloudbeds or CapU systems must use strong passwords and, where applicable, MFA for added security.
- Audit Logs & Monitoring:
    - All access to personal information is logged and monitored, tracking who accessed, modified, or updated records and when.
    - Regular security audits are conducted to detect unauthorized access attempts.
- Encryption & Secure Data Storage:
    - Cloudbeds encrypts personal data at rest and in transit to prevent interception.
    - Financial data (e.g., credit card information) is tokenized and handled by a PCI DSS-compliant payment processor—CapU does not store credit card details.

2. Physical Security Measures (For Paper Records & On-Site Systems)

- Locked Storage for Paper Records:
    - If any personal information is stored in paper format (e.g., contracts, invoices), it is kept in locked cabinets with restricted access.
    - Physical access is limited to authorized personnel only.
- Key Card & Restricted Access to Workstations:
    - Workstations with access to personal information are restricted to authorized employees via key card entry.
    - Auto-locking mechanisms ensure computers are locked after periods of inactivity.
- Secure Disposal of Records:
    - Paper-based records are digitized and securely shredded once they are no longer needed.
    - Digital records are permanently deleted after their retention period expires.

3.Preventing Unauthorized External Access

- No Unauthorized Data Sharing:
    - Personal information is not shared with third-party vendors unless required for payment processing or legal compliance.
    - Any third-party access (e.g., Cloudbeds, Stripe/PayPal) is monitored and contractually bound to data protection agreements.
- Strict Compliance with FIPPA & Cloudbeds Security Policies:
    - Data stored in Amazon AWS (US-West-2 Region) follows local privacy laws and compliance standards.

No unauthorized international transfers without explicit approval.

More security information is provided here: Cap U Security Questions - Google Docs

    -

If there is a third party or a service provider involved in the initiative, what access controls are/will be put in place?

Third-Party/Service Provider Access Controls

Yes, third-party service providers are involved in the initiative, primarily Cloudbeds for booking management and Stripe/PayPal for payment processing. Strict access controls are in place to protect personal information.

1. Cloudbeds (Booking & Data Management System)

- Role-Based Access Control (RBAC):
  - Only authorized CapU staff (e.g., reservations, finance teams) have access to Cloudbeds based on their job function.
  - Access is tiered, ensuring employees can only view or modify data necessary for their role.
- Encryption & Secure Storage:
  - Cloudbeds encrypts all personal information at rest and in transit.
  - Financial data (credit card info) is not stored by CapU; it is handled by Cloudbeds' PCI DSS-compliant payment processor.
- Audit Logging & Monitoring:
  - Cloudbeds tracks all user actions, logging who accessed, modified, or exported data.
  - Regular audits help detect unauthorized access or suspicious activity.
- Limited External Data Sharing:
  - Cloudbeds does not share personal information with other parties unless required for payment processing or legal compliance.

2. Payment Processors (Stripe, PayPal, or Other PCI DSS-Compliant Providers)

- Tokenized Transactions:
  - CapU does not store or handle raw credit card data—all transactions are securely processed by a third-party PCI DSS-compliant provider.
  - Payment details are tokenized, ensuring sensitive financial data is not accessible within Cloudbeds.
- Fraud Detection & Compliance:
  - Stripe/PayPal monitor transactions for fraud and unauthorized access.
  - Payment data is handled in compliance with Canada’s privacy laws, PCI DSS, and FIPPA.

3. CapU Internal Access Controls for Third-Party Systems

- Secure Login & Authentication:
  - Multi-Factor Authentication (MFA) is required for CapU administrators accessing Cloudbeds.
  - Strong password policies and auto-logout features prevent unauthorized access.
- Restricted Third-Party Access:
  - No external vendors or marketing partners can access Cloudbeds without explicit approval.
  - Any potential integration (e.g., analytics tools) must comply with CapU’s data privacy policies.
- Legal Agreements & Compliance:
  - Cloudbeds and payment providers are contractually required to:
    - Comply with FIPPA, PCI DSS, and other applicable regulations.
    - Ensure secure storage and limited data access.
    - Allow CapU to audit data security measures if needed.

2. Disclosure of Personal Information:			
Please respond to the following statements:	**YES**	**NO**	**N/A**
Will personal information be disclosed internally to an employee, only when the information is necessary for the performance of the duties of that employee?	☒	☐	☐
Personal information will only be accessed by CapU employees on a need-to-know basis to perform their job functions, such as managing reservations, processing payments, and coordinating event logistics. Role-based access controls (RBAC) ensure that only authorized personnel can access specific data.			
Will the personal information be disclosed externally to a service provider, only when the information is necessary for the delivery of the contracted services?	☒	☐	☐
Personal information will be disclosed externally only when necessary, primarily to: • Cloudbeds (for booking management and secure data storage). • Third-party PCI DSS-compliant payment processors (e.g., Stripe, PayPal) for secure payment transactions. • Regulatory authorities (if legally required) for compliance or audit purposes. All disclosures align with FIPPA and data protection policies to ensure privacy and security.			

3. Storage of Personal Information: *Describe exactly where and how will the personal information be stored.*	
WHERE? *e.g., in Canada or outside Canada? Provide details.*	Data is stored in AWS's US-West-2 Region (not Canada). AWS follows PCI DSS, GDPR, and other international data security standards and follows applicable local privacy and compliance regulations. In this case, it follows the Oregon Privacy Act which is comparable to California privacy standards.
HOW/WHAT FORMAT? *e.g., electronic, and on-premise servers or data centres.*	Electronic format in cloud storage

D. ACCURACY, CORRECTION, RETENTION & DISPOSAL OF PERSONAL INFORMATION

1. Decisions Affecting Individuals (Section 28):		
	YES	**NO**
As part of this initiative, an individual's personal information will be used to make a decision that directly affects the individual.	☒	☐
Examples of using personal information to make decisions include but are not limited to: • *Using a person's employment history to decide whether they can move forward in a job competition* • *Using a student's exam results to pass them in a course*		

- *Using a student's information to approve them for financial aid*

If "yes", please explain how and why that will be done:

How and Why Personal Information Will Be Used for Decision-Making:

1. **Room & Venue Booking Approval**
    a. Personal information (e.g., name, contact details, booking request details) will be used to determine:
        i. Whether a requested room/venue is available for the specified date.
        ii. If the request meets booking criteria (e.g., eligibility for certain groups or types of events).
        iii. The confirmation or denial of a reservation based on capacity and scheduling.
2. **Payment Processing & Invoicing**
    a. Financial information (e.g., invoicing details, billing address) will determine:
        i. Whether a payment is successfully processed for the booking.
        ii. If a booking should be confirmed, canceled, or placed on hold due to payment status.
3. **Group & Conference Bookings**
    a. If a booking is for a conference or special event, personal and organizational details may be reviewed to:
        i. Assess if the request aligns with university policies and event criteria.
        ii. Determine pricing, available discounts, or custom requirements.
4. **Security & Compliance Checks (If Required)**
    a. Some high-profile or external event bookings may require additional review to ensure:
        i. Compliance with university policies and security protocols.
        ii. Appropriate permits, insurance, or approvals are in place before confirming a booking

5. **Safeguards to Ensure Fair & Accurate Decision-Makin**g:

- All decisions are based on verified information collected directly from the individual.
- Automated confirmation emails allow individuals to review and correct any errors before finalizing a booking.
- Role-based access controls (RBAC) ensure only authorized personnel make booking-related decisions.
- Appeal & correction process: If an error impacts an individual's booking, they can contact CapU staff to request corrections or further review.

All decisions made using personal information will follow established procedures, ensuring transparency, fairness, and compliance with FIPPA.

If answered "yes" above, please respond to the following statement:

Public bodies are required to keep personal information for a minimum of one year after it is used to make a decision that affects the individual.
Please describe how/what steps will be taken to ensure the information will be kept for a minimum of one year after it's used to make a decision that directly affects an individual.

To comply with FIPPA requirements, personal information used in booking decisions will be retained for at least one year after the decision is made. The following measures will ensure compliance:

1. Retention Policy Implementation

- All booking records, approvals, and related correspondence will be stored in Cloudbeds and retained for a minimum of one year after the final decision (e.g., approval, cancellation, or modification).
- Financial records and invoices will be stored separately per financial compliance policies but will also be available for reference for at least one year.

2. System-Managed Record Retention (Cloudbeds & Internal Storage)

- Cloudbeds automatically retains booking records and payment transactions for reference.
- CapU's internal file management system ensures that any manually entered records (e.g., group booking forms, contract approvals) remain stored securely.

3. Controlled Access & Archiving

- Role-based access controls (RBAC) will be in place to ensure only authorized personnel can access past decisions.
- After one year, records will be reviewed and either archived for compliance or securely deleted per data retention policies.

4. Secure Record Disposal After Retention Period

- Once the required one-year retention period is met:
  - Electronic records will be securely deleted from the system.
  - Paper records (if applicable) will be securely shredded after digitization.
  - Financial records will be retained per applicable tax/audit regulations beyond the one-year requirement.

These steps ensure compliance with FIPPA's minimum retention requirements while maintaining data security and integrity.

2. Accuracy of Personal Information (Section 28):
If an individual's personal information is used to make a decision that directly affects that individual, please explain the efforts that will be made to ensure that the personal information is accurate and complete (e.g., collecting the information directly from the individual, verifying the information with the individual prior to recording it, etc.).

Accuracy of Personal Information (Section 28 – FIPPA Compliance)

1. **Direct Collection from the Individual**

    a. Personal information is collected directly from the individual via:
        i. CapU's booking inquiry website (for room and venue requests)
        ii. Cloudbeds online booking system (for room reservations)
        iii. Direct phone/email inquiries (entered manually by CapU staff for group/conference bookings)

2. V**erification Before Recording**

    a. When an inquiry is received, CapU staff:
        i. Reviews the information for completeness.

ii. Confirms key details (e.g., booking dates, contact details) with the individual before entering them into Cloudbeds.

b. If a booking is made manually (e.g., phone inquiry), the individual receives a confirmation email where they can review and correct details before finalization.

3. Confirmation & Review by the Individual

a. Automated confirmation emails from Cloudbeds allow individuals to:
   i. Review the accuracy of their booking details.
   ii. Identify any errors in personal information (e.g., incorrect dates, contact details).
   iii. Notify CapU staff if corrections are needed.

4. Identity Verification for Critical Changes

a. If changes are requested for sensitive information (e.g., name corrections, payment details), CapU staff will:
   i. Verify the requester's identity before making updates.
   ii. Require official documentation (if applicable) for significant changes.

5. Regular Audits & Data Validation

a. Periodic internal audits will be conducted to review:
   i. Booking records for inconsistencies.
   ii. Contact details to ensure active email/phone numbers.

b. Staff will flag and resolve discrepancies proactively.

6. Final Review Before Decision-Making

a. If an individual's information is used in decision-making processes (e.g., eligibility for accommodations, invoicing, or event approvals), a final review will be conducted to ensure all details are accurate and complete.

3. Correction of Personal Information (Section 29):
Please describe how an individual can update or correct their personal information. Describe the process, this could be processes where an individual can ask for system administrators to make changes on their behalf.

Correction of Personal Information (Section 29 – FIPPA Compliance)

Individuals will have the ability to update or correct their personal information through a structured process to ensure accuracy and compliance with FIPPA.

Process for Updating or Correcting Personal Information:

1. Direct Update via Cloudbeds (If Applicable)

- If the individual has access to their Cloudbeds profile, they may log in and update certain details, such as:
  - Contact information (email, phone number)
  - Address (if applicable)
  - Communication preferences

- Some fields, like payment details, are securely managed by the payment processor and cannot be edited directly by the user.

2. Requesting Updates via CapU Staff

If an individual needs to correct personal information that they cannot update themselves, they can submit a request through the following methods:

- **Email Inquiry:**
  - Individuals can send a request to the CapU reservations team (designated email or contact).
  - The request should include:
    - Full name
    - Booking reference number (if applicable)
    - Details of the requested correction
- **Phone Inquiry:**
  - Guests may call the reservations team to request updates.
  - Staff will verify the individual's identity before making any changes.

3. Verification & Processing of the Correction Request

- To prevent unauthorized changes, CapU staff will verify the requester's identity before modifying any details.
- Once verified, a system administrator or authorized staff member will update the information in Cloudbeds.
- A confirmation email will be sent to the individual once the update is completed.

4. Financial Information Corrections

- Credit card details cannot be edited by CapU staff, as they are securely handled by the third-party payment processor.
- If payment details need to be updated, the individual must re-enter new payment information at the time of booking or contact the payment processor directly.

5. Timeline for Processing Corrections

- Standard requests for non-sensitive information (e.g., phone number, address) will be processed within 3 business days.
- Corrections requiring higher-level verification (e.g., name changes, official documents) may take 5-7 business days.

If it is not possible to update or correct the information (for physical, procedural, or other reasons) please explain how it will be annotated to reflect that the correction was requested but not made.

In the case information cannot be corrected, the booking cannot be completed and will need to be redone with accurate information.

Where personal information is disclosed to third parties, how will the third parties be notified of the update, correction, or annotation?

Notifying Third Parties of Updates, Corrections, or Annotations to Personal Information

If personal information has been disclosed to a third party (e.g., Cloudbeds, payment processors), the following process will be used to ensure they are notified of any updates, corrections, or annotations:

1. Identifying Third-Party Data Recipients

- Before updating or correcting personal information, CapU will review where the data has been shared (e.g., Cloudbeds for booking records, Stripe/PayPal for payments).
- A record of disclosures will be maintained to track any instances where third parties received personal data.

2. Notification Process for Updates & Corrections

- Cloudbeds (Booking & Reservation System):
  - Updates made within Cloudbeds (e.g., name corrections, contact details) will automatically reflect in the system and will not require external notification.
  - If a correction affects invoices or financial records, CapU staff will ensure adjustments are reflected in both Cloudbeds and financial processing systems.
- Payment Processors (Stripe, PayPal, etc.):
  - If an individual requests a correction related to billing details, CapU will instruct the individual to update their information directly with the payment processor (as CapU does not store or control payment details).
  - If an incorrect charge occurred due to an error in personal information, CapU will process an adjustment and notify the payment processor accordingly.

3. Documentation & Confirmation of Updates

- CapU will keep a record of any updates made to personal information that required third-party notification.
- Individuals will receive confirmation once their data has been corrected and any necessary updates have been communicated to relevant third parties.

4. Ongoing Compliance & Audit Logs

- All updates and corrections are logged to ensure compliance with FIPPA.
- CapU staff will review third-party data retention policies to confirm they align with privacy obligations.

This process ensures that any corrections to personal information are reflected across all systems where the data was previously shared, maintaining accuracy and compliance.

To be completed by the Privacy Officer:

s. 29	Right to request correction of personal information	YES	NO	N/A
	Are there procedures in place to enable an individual to request/review a copy of their own personal information?	☒	☐	☐

(1), (2)	Are there procedures in place to correct or annotate an individual's personal information if requested, including the source that was used to update the file?	☒	☐	☐
(3)	Is there a process in place to notify third parties where a correction is requested?	☒	☐	☐
	Do controls and procedures exist for the authority to add, change, or delete personal information?	☒	☐	☐
	Are reasonable efforts taken to ensure that personal information is accurate and complete if being used to make a decision that directly affects the individual?	☒	☐	☐

4. Records Retention (Section 31):
Personal information collected, used, and/or disclosed as part of this initiative must have an assigned retention period. Is there a defined retention period assigned? How long the records will be retained for?

Retention Periods for Different Data Types

Type of Record	Retention Period	Reason for Retention
Booking Records (Guest Profiles, Reservation Details, Contact Information)	2 years after the last interaction	To facilitate repeat bookings and customer service support
Financial Records (Invoices, Receipts, Payment Transactions – Excluding Credit Card Data)	7 years	Compliance with financial and tax regulations
Credit Card Information	Not stored (Tokenized & handled by third-party processor)	PCI DSS compliance – no financial data is retained by CapU
Contracts & Agreements (Venue Rentals, Event Bookings, Signed Documents)	7 years	Legal and audit compliance
Marketing & Communications Data (If consented by the user)	Until user opts out or 2 years of inactivity	CASL compliance – ensures individuals can opt out anytime
System Access & Audit Logs	1 year	Security monitoring and audit trail for compliance
Paper-Based Records (If applicable)	Retained as per corresponding category, then securely shredded	To align with digital record retention

Final Disposition of Records

- Electronic records are permanently deleted after their retention period expires.
- Paper records are securely shredded once their retention period is met.
- Personal information will not be retained longer than necessary and will be securely disposed of following CapU's data retention policies.

These retention periods align with legal, financial, and operational requirements while ensuring compliance with FIPPA.

5. Disposal

How are the records containing personal information disposed of?
Who (title) is in charge of disposing them?

Records containing personal information are disposed of securely following CapU's data retention policies and in compliance with FIPPA.

1. Disposal of Electronic Records

- Cloudbeds automatically deletes records once they reach the end of their retention period.
- Financial records and invoices stored within CapU's internal systems are securely deleted in accordance with financial compliance regulations.
- Audit logs and system access records are retained for a defined period before being permanently deleted.
- Payment details are never stored by CapU—third-party payment processors handle financial transactions and remove records as per PCI DSS guidelines.

2. Disposal of Paper Records (If Applicable)

- Paper records (e.g., contracts, invoices, booking confirmations) are digitized and securely shredded once their retention period has expired.
- Shredding is conducted using cross-cut shredders or secure document disposal services.

3. Responsible Party for Disposal

The CapU Records Management Team is responsible for overseeing the secure disposal of personal information, with the following roles involved:

- Records Administrator: Ensures compliance with retention schedules and oversees the secure deletion of digital records.
- IT Security & Compliance Officer: Manages secure data deletion within Cloudbeds and other CapU systems.
- Finance Department (For Financial Records): Oversees the secure disposal of invoices and transaction history in accordance with tax laws.

These procedures ensure that personal information is disposed of securely, preventing unauthorized access or misuse.

E. ACCESS, DISCLOSURE, STORAGE, RETENTION & DISPOSAL OF SENSITIVE PERSONAL INFORMATION OUTSIDE OF CANADA

Complete this section only if you are disclosing or storing sensitive personal information outside of Canada. Please contact the Privacy Officer for assistance.

To be completed by the Privacy Officer:		
	YES	NO
Is it necessary to fill out section E. of this PIA?	☒	☐

1. Is Sensitive Personal Information Disclosed Outside of Canada under FIPPA section 33(2)(f)?
FIPPA Section 33(2)(f) states that a public body may disclose personal information if the information is made available to the public under an enactment that authorizes or requires the information to be made public.

Sensitive personal information will be stored outside of Canada.

Please respond to the following statements:	YES	NO	N/A
Is access to sensitive personal information based on a need-to-know basis?	☒	☐	☐
If you're utilizing third party for storage/processing of sensitive personal information, do you have controls in place to monitor access?	☒	☐	☐
Is there an ongoing audit process that can track access (e.g., who accessed and/or updated sensitive personal information records and when)?	☒	☐	☐

2. Access to Sensitive Personal Information:
Identify who will have access to sensitive personal information as a result of this project (e.g., teams, roles, or individuals, including any third party service providers, contractors, etc.), what type of sensitive personal information will they be privy to, the purposes for which they will have access, and how information will be made available to them/user access assigned?

Who?	Type of PI?	Purpose(s)?	How?
Manager - Student Housing, Squamish	**Full access: Name, phone number, email, tokenized credit card information, address**	**This information is necessary to manage bookings and communicate with guests who have booked accommodations.**	**Web-based application**
Director, Student Housing and Food Services	**Full access: Name, phone number, email, credit card information, address**	**This information is necessary as the director will handle the above manager's job duties until a manager is hired into the position. After this, the director will need access to the Cloudbeds system to adequately train the new manager or**	**Web-based application**

		assist duties if the manager is away.	
Manager, Community Engagement and Events	**Full access for back-end setup**	**Will be setting up the back end of the Cloudbeds booking system and working with the new manager for conference bookings.**	**Web-based application**
Housing Staff	**Names, room numbers, check-in/checkout dates, basic contact information**	**Need information regarding reservations to assist guests, prepare rooms for accommodations, etc.**	**Web-based application**

Provide details about how you will track and monitor access to sensitive personal information (e.g., audit trails or physical sign-in and sign-out of files)?

The Cloudbeds system has audit trails to track access to the system and sensitive data.

Is there a defined approval process in place for granting access? Is there a person (title) who will authorize and/or revoke access? How/how often will the approval authorities be reviewed to ensure they are current?

The Manager, Student Housing Services, Squamish will be responsible for granting access to employees who need access.

Identify who (title) has the authority to add, change or delete sensitive personal information. Is this power limited to a specific individual(s) or anyone with access can add, change, or delete personal information?

The Manager, Student Housing Services, Squamish will be responsible for granting/removing access to employees who need access.

What controls are in place to prevent unauthorized access to sensitive personal information (e.g., locked cabinets, key cards, passwords)?

Cloudbeds and CapU have multiple security measures in place to protect personal information from unauthorized access.

1. Electronic Data Security (Cloudbeds & CapU Systems)

- Role-Based Access Control (RBAC):
  - Only authorized personnel (e.g., reservations team, finance staff) have access to personal information.
  - Users are granted the minimum level of access required for their role.
- Password Protection & Multi-Factor Authentication (MFA):
  - Staff accessing Cloudbeds or CapU systems must use strong passwords and, where applicable, MFA for added security.
- Audit Logs & Monitoring:
  - All access to personal information is logged and monitored, tracking who accessed, modified, or updated records and when.
  - Regular security audits are conducted to detect unauthorized access attempts.
- Encryption & Secure Data Storage:
  - Cloudbeds encrypts personal data at rest and in transit to prevent interception.

- Financial data (e.g., credit card information) is tokenized and handled by a PCI DSS-compliant payment processor—CapU does not store credit card details.

2. Physical Security Measures (For Paper Records & On-Site Systems)

- Locked Storage for Paper Records:
  - If any personal information is stored in paper format (e.g., contracts, invoices), it is kept in locked cabinets with restricted access.
  - Physical access is limited to authorized personnel only.
- Key Card & Restricted Access to Workstations:
  - Workstations with access to personal information are restricted to authorized employees via key card entry.
  - Auto-locking mechanisms ensure computers are locked after periods of inactivity.
- Secure Disposal of Records:
  - Paper-based records are digitized and securely shredded once they are no longer needed.
  - Digital records are permanently deleted after their retention period expires.

3.Preventing Unauthorized External Access

- No Unauthorized Data Sharing:
  - Personal information is not shared with third-party vendors unless required for payment processing or legal compliance.
  - Any third-party access (e.g., Cloudbeds, Stripe/PayPal) is monitored and contractually bound to data protection agreements.
- Strict Compliance with FIPPA & Cloudbeds Security Policies:
  - Data stored in Amazon AWS (US-West-2 Region) follows local privacy laws and compliance standards.

No unauthorized international transfers without explicit approval.

If there is a third party or a service provider involved in the initiative, what access controls are/will be put in place?

Third-Party/Service Provider Access Controls

Yes, third-party service providers are involved in the initiative, primarily Cloudbeds for booking management and Stripe/PayPal for payment processing. Strict access controls are in place to protect personal information.

1. Cloudbeds (Booking & Data Management System)

- Role-Based Access Control (RBAC):
  - Only authorized CapU staff (e.g., reservations, finance teams) have access to Cloudbeds based on their job function.
  - Access is tiered, ensuring employees can only view or modify data necessary for their role.
- Encryption & Secure Storage:
  - Cloudbeds encrypts all personal information at rest and in transit.
  - Financial data (credit card info) is not stored by CapU; it is handled by Cloudbeds' PCI DSS-compliant payment processor.
- Audit Logging & Monitoring:
  - Cloudbeds tracks all user actions, logging who accessed, modified, or exported data.

- Regular audits help detect unauthorized access or suspicious activity.
- Limited External Data Sharing:
  - Cloudbeds does not share personal information with other parties unless required for payment processing or legal compliance.

2. Payment Processors (Stripe, PayPal, or Other PCI DSS-Compliant Providers)

- Tokenized Transactions:
  - CapU does not store or handle raw credit card data—all transactions are securely processed by a third-party PCI DSS-compliant provider.
  - Payment details are tokenized, ensuring sensitive financial data is not accessible within Cloudbeds.
- Fraud Detection & Compliance:
  - Stripe/PayPal monitor transactions for fraud and unauthorized access.
  - Payment data is handled in compliance with Canada's privacy laws, PCI DSS, and FIPPA.

3. CapU Internal Access Controls for Third-Party Systems

- Secure Login & Authentication:
  - Multi-Factor Authentication (MFA) is required for CapU administrators accessing Cloudbeds.
  - Strong password policies and auto-logout features prevent unauthorized access.
- Restricted Third-Party Access:
  - No external vendors or marketing partners can access Cloudbeds without explicit approval.
  - Any potential integration (e.g., analytics tools) must comply with CapU's data privacy policies.
- Legal Agreements & Compliance:
  - Cloudbeds and payment providers are contractually required to:
    - Comply with FIPPA, PCI DSS, and other applicable regulations.
    - Ensure secure storage and limited data access.

Allow CapU to audit data security measures if needed.

3. Disclosure of Sensitive Personal Information:			
Please respond to the following statements:	**YES**	**NO**	**N/A**
Will the sensitive personal information be disclosed internally to an employee, only when the information is necessary for the performance of the duties of that employee? Sensitive personal information will be disclosed externally only when necessary, specifically to: • Cloudbeds (for managing bookings, customer profiles, and invoices). • Third-party PCI DSS-compliant payment processors (e.g., Stripe, PayPal) to securely process financial transactions. No other third parties will receive sensitive information unless legally required (e.g., tax audits, compliance requests).	☒	☐	☐

Will the information be disclosed externally to a service provider, only when the information is necessary for the delivery of the contracted services?	☒	☐	☐

4. Storage of Sensitive Personal Information:		
Please respond to the following question:	**YES**	**NO**
Sensitive personal information is stored within Cloudbeds, which hosts data on Amazon AWS (US-West-2 Region) and follows PCI DSS-compliant encryption standards. • CapU does not store or retain credit card information—all financial transactions are handled securely by third-party payment processors. • Sensitive personal data is encrypted both at rest and in transit to prevent unauthorized access. These safeguards ensure compliance with FIPPA and data protection policies.	☒	☐

If "yes", fill in the table below:	
Name of the Service Provider:	Cloudbeds
Name of cloud infrastructure and/or platform provider(s) (if applicable):	Cloudbeds utilizes Amazon Web Services (AWS) as its cloud infrastructure provider. • Compliance: AWS follows PCI DSS, GDPR, and other international data security standards. • Data Protection: Cloudbeds encrypts data at rest and in transit using AWS security protocols
Where is the sensitive personal information stored (including backups):	Data is stored in AWS's US-West-2 Region (not Canada). AWS follows PCI DSS, GDPR, and the other international data security standards and applicable local privacy and compliance regulations. In this case, it follows the Oregon Privacy Act which is comparable to California privacy standards.

If "no", please provide the details of the disclosure: *Please include to whom is the sensitive personal information disclosed to, and where is it stored:*
N/A
5. Records Retention (Section 31): *Personal information collected, used, and/or disclosed as part of this initiative must have an assigned retention period. Is there a defined retention period assigned? How long the records will be retained for?*
As stated in section C, guest information is collected when a reservation is made in the system. It is retained until the reservation has ended and 30 days have passed. At this point all guest information is deleted from the system. The only exception is when a user opts in to further

marketing communication, in which case contact information is retained indefinitely until the user opts-out of communications.

6. Disposal
How are the records containing personal information disposed of?
Who (title) is in charge of disposing them?

As stated above in section C, the system deletes guest personal information automatically once the retention period is over. Contact information is kept indefinitely if opted into marketing info until opt-out requested, at which point contact information is deleted.

To be completed by the Privacy Officer:

7. Privacy Risks:
Describe the privacy risks for disclosure of sensitive personal information outside of Canada. What about metadata, data in transit and at rest? Is any data routed outside of Canada?

Use the table below to outline the risk associated with unauthorized collection, use, disclosure, or storage of sensitive personal information, when disclosure is made outside of Canada. Include a description of the potential impacts (consider both individuals and any broader impact if relevant) and then rate the likelihood and the level of risk (use a simple low, medium high scale). For each privacy risk identified describe the current controls and those that will be put in place as part of the initiative. Controls may include contractual, technical, security, administrative and/or policy measures. Where the level of risk is still significant describe the additional controls that need to be implemented.

Area of Risk Exposure	Likelihood	Impact	Level of Privacy Risk	Mitigation Strategy / Actions	Responsibility for Mitigation Actions	Timeline for Mitigation Actions
Unauthorized employees or individuals could access the personal information in the system and use or disclose it for personal purposes	Low	High	Med	Employee code of conduct, privacy policy, and privacy training in place to prevent unauthorized use of PI. Access to system requires credentials and password. Computers with access to system will be in locked rooms.	CapU Student Residence Staff	Ongoing Mitigation – Prevention before breaches; any breaches will be responded to immediately following University procedure.

Unauthorized individuals at Cloudbeds could access PI	Low	High	Med	Employees of Cloudbeds are required to act in a manner consistent with their privacy policy and client agreement. Furthermore, they will not have access to CapU PI without consent and monitoring of program area administrators.	Cloudbeds staff, CapU Student Residences Staff	Ongoing Mitigation – Prevention before breaches; any breaches will be responded to immediately following Cloudbeds and then University procedure.
Privacy breach of Cloud Storage	Low	High	Med	AWS to inform Cloudbeds immediately, then Cloudbeds would inform CapU. Initiate breach response procedure from AWS, Cloudbeds, and CapU.	AWS staff, Cloudbeds staff, CapU staff	Immediately after breach is found

The outcome of Section E. will be a risk-based decision made by the project sponsors in consultation with the Privacy Officer and cybersecurity manager as to whether to proceed with the initiative as planned or to proceed only if additional risk-reducing controls are implemented. If the privacy risk is determined to be too significant, alternatives will need to be explored.

F. RISK MANAGEMENT & SECURITY OF PERSONAL INFORMATION

1. Protection of Personal Information (Section 30):
Describe the audit, compliance, and enforcement mechanisms in place to protect against the unauthorized collection, access, use, disclosure, or storage of personal information, in course of the initiative (including for contracted service providers).

Cloudbeds and CapU have multiple security measures in place to protect personal information from unauthorized access.

1. Electronic Data Security (Cloudbeds & CapU Systems)

- Role-Based Access Control (RBAC):
  - Only authorized personnel (e.g., reservations team, finance staff) have access to personal information.
  - Users are granted the minimum level of access required for their role.
- Password Protection & Multi-Factor Authentication (MFA):
  - Staff accessing Cloudbeds or CapU systems must use strong passwords and, where applicable, MFA for added security.
- Audit Logs & Monitoring:

- All access to personal information is logged and monitored, tracking who accessed, modified, or updated records and when.
- Regular security audits are conducted to detect unauthorized access attempts.

- Encryption & Secure Data Storage:
  - Cloudbeds encrypts personal data at rest and in transit to prevent interception.
  - Financial data (e.g., credit card information) is tokenized and handled by a PCI DSS-compliant payment processor—CapU does not store credit card details.

2. Physical Security Measures (For Paper Records & On-Site Systems)

- Locked Storage for Paper Records:
  - If any personal information is stored in paper format (e.g., contracts, invoices), it is kept in locked cabinets with restricted access.
  - Physical access is limited to authorized personnel only.
- Key Card & Restricted Access to Workstations:
  - Workstations with access to personal information are restricted to authorized employees via key card entry.
  - Auto-locking mechanisms ensure computers are locked after periods of inactivity.
- Secure Disposal of Records:
  - Paper-based records are digitized and securely shredded once they are no longer needed.
  - Digital records are permanently deleted after their retention period expires.

3.Preventing Unauthorized External Access

- No Unauthorized Data Sharing:
  - Personal information is not shared with third-party vendors unless required for payment processing or legal compliance.
  - Any third-party access (e.g., Cloudbeds, Stripe/PayPal) is monitored and contractually bound to data protection agreements.
- Strict Compliance with FIPPA & Cloudbeds Security Policies:
  - Data stored in Amazon AWS (US-West-2 Region) follows local privacy laws and compliance standards.

No unauthorized international transfers without explicit approval.

2. Policies and Procedures:

Are there policies and procedures in place for the security of personal information during routine collection, use and disclosure of the information? How will these be communicated to necessary parties, including employees, contractors, and third party service providers?

B.604 Acceptable Use and Security of Digital Technology Policy

B.700 Privacy and Access to Information Policy

B.700.1 Personal Information Incident Management Procedure

OP.608 Password Policy

Cloudbeds has its own privacy and information security policies

Cloudbeds system is FIPPA and CASL compliant

3. Training:

Please describe how the conditions detailed in this PIA will be communicated to necessary parties, including employees, contractors, and third party service providers? Will specific guidance or training be provided on how to handle personal information in a privacy protective manner? Where you rely on enterprise-led privacy awareness training alone, please indicate this.

CapU Housing staff all complete University FOI and privacy protection training.

Cloudbeds staff undergo proprietary privacy training.

4. Privacy Incident Reporting:

Please describe how necessary parties, including employees, contractors, and third party service providers, will be made aware of the privacy incident notification process (as documented in the University's "Personal Information Incident Management Procedure").

This initiative would follow the steps identified within B.700.1 Personal Information Incident Management Procedure.

5. Contract:

Has there been a contract drafted or signed? If so, please indicate below and provide a copy to the Privacy Officer.

In lieu of a contract or service agreement, University staff have agreed to the Cloudbeds Terms of Service during product purchase.

6. Contractual Privacy Provisions: [To be completed by Privacy Officer]

If the contract has been drafted or signed, does it include privacy provisions?

The Terms of Service reference the Cloudbeds Privacy Policy. Cloudbeds does not collect PI that is provided by customers' booking at specific venues, but it does collect limited data from users who visit the Cloudbeds website, communications data, and publicly available information shared to social media. Furthermore, the use and disclosure of information collected is clearly stated. Upon review, the Cloudbeds Privacy Policy aligns with best practices and reserves the right to collect reasonable amounts of data and personal information. A copy of the Terms of Service and the Privacy Policy at the time of signing is attached as appendices in this PIA.

7. Risk Reduction:

How will you (and the third party providers, if applicable) reduce the risk of unintentionally collecting personal information?

For example, if you are collecting opinions as part of a public engagement strategy, participants may offer personal information about themselves or others, even though you've instructed them not to. If you do inadvertently receive or collect personal information, what steps will you take to:

- *Destroy it*
- *Return it*
- *Transfer it to the correct recipient*

Guests who are booking a reservation will be provided with limited options to enter information into the system. In the event that PI is unintentionally collected, that information will be deleted from the system.

8. Digital Tools, Databases, or Information Systems:

A digital tool, database or information system may leave personal information exposed or otherwise vulnerable to security threats.

	YES	NO
Does your initiative involve digital tools, databases, or information systems?	☒	☐

If "yes", please describe:

Cloudbeds is a digital tool that manages multiple accommodations bookings.

To be completed by the Privacy Officer:

9. STRA (Security Threat and Risk Assessment):

Security assessments are used on information systems and other digital tools to assess and document security risks, risk ratings and planned risk responses. If a security assessment will be completed during the development of the initiative, the questions about technical security in this PIA template do not need to be completed. Instead, once the assessment has been finished it should be attached to the template.

	YES	NO
Will a separate security assessment be completed?	☒	☐

If "yes", please describe the assessment to be undertaken, including who will complete the assessment and when it will be completed:

STRA was completed and approved by Michael Shi on 29-Mar-2025. Risks identified has low to medium risk ratings and recommendations for mitigation were included.

10. Physical Security Measures:

Please describe the physical security measures established to protect the personal information in all media forms from unauthorized access.

Describe all aspects of the physical environment where personal information is held (e.g., Server(s) location/security, key card access to offices, CCTV surveillance, shredding, locked cabinets, password encryption for computers/laptops, alarm systems, building protection, staff screening, onsite security personnel, etc.).

Computers that will be used to access Cloudbeds system are in a secure area with locked doors. The area is secured with video surveillance, keycards, etc. Computers themselves are password protected, etc.

10. Technical Security Measures:

Please describe the technical security measures established to protect the personal information in transit, at rest, and while in use.

Please list the specific technical security measures in place to protect personal information and provide as much detail as possible (e.g., Firewall/virus protection and monitoring, tokenization, web interface

features, encryption, backup cycles, scan software, VPN protocols, password protection, audits, role-based access, etc.).
Firewalls, virus protection, encryption, MFA, password protection, PCI is tokenized.

To be completed by the Privacy Officer:		
	YES	**NO**
Is there reasonable technical security in place to protect against unauthorized access or disclosure?	☒	☐
Is there reasonable physical security in place to protect against unauthorized access or disclosure?	☒	☐

To be completed by the Privacy Officer:		
11. a) Data-linking Initiative:		
Please respond to the following statements:	**YES**	**NO**
Personal information from one database will be linked or combined with personal information from another database.	☐	☒
The purpose for the linkage is different from that for which the personal information in each database was originally obtained or compiled.	☐	☒
Data linking will occur between either (i) two or more public bodies or (ii) one or more public bodies and one or more agencies.	☐	☒
11. b) Based on the answers above, 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.*		
This initiative does not involve data linking as identified in FIPPA.		

To be completed by the Privacy Officer:		
12. a) Common or Integrated Program or Activity:		
Please respond to the following statements:	**YES**	**NO**
This initiative involves a program or activity that provides a service (or services) to the public.	☐	☒
Those services will be provided through (i) a public body and at least one other public body or agency working collaboratively to provide that service or (ii) one public body working on behalf of one or more other public bodies or agencies.	☐	☒
There is a written agreement signed by the head of each public body and agency through which the services of the program or activity are provided.	☐	☒
12. b) Based on the answers above, is this initiative a common or integrated program or activity? *Under section FIPPA 69(5.4), you must submit this PIA to the Office of the Information and Privacy Commissioner.*		

This initiative is not a common/integrated program as defined by FIPPA.

To be completed by the Privacy Officer:		
13. a) Project with High Visibility/Public Interest, and/or Audio/Video Surveillance:		
Please respond to the following statements:	**YES**	**NO**
This initiative involves installation or use of audio recording equipment.	☐	☒
This initiative involves installation or use of video recording equipment.	☐	☒
This initiative involves the use of new technology which might be perceived as being privacy intrusive. For example, the use of biometrics or facial recognition.	☐	☒
This initiative involves a program or activity that may generate high visibility or public interest.	☐	☒
13. b) Based on the answers above, does this initiative qualify as a project with high visibility/public interest, and/or does it include audio or video surveillance? *If so, the completed PIA should be sent to the OIPC for review and comment.*		
This will not be an initiative with new audio/visual surveillance or of high public interest because of privacy intrusive activities.		

To be completed by the Privacy Officer:

14. Privacy Risks:

Use the table below to outline the risk associated with unauthorized collection, use, disclosure, or storage of personal information. Include a description of the potential impacts (consider both individuals and any broader impact if relevant) and then rate the likelihood and the level of risk (use a simple low, medium & high scale). For each privacy risk identified describe the current controls and those that will be put in place as part of the initiative. Controls may include contractual, technical, security, administrative and/or policy measures. Where the level of risk is still significant describe the additional controls that need to be implemented.

Area of Risk Exposure	Likelihood	Impact	Level of Risk	Mitigation Strategy / Actions	Responsibility for Mitigation Actions	Timeline for Mitigation Actions
Unauthorized employees or individuals could access the personal information in the system and	Low	High	Med	Employee code of conduct, privacy policy, and privacy training in place to prevent unauthorized use of PI. Access to system requires credentials and password. Computers with access to	CapU Student Residence Staff	Ongoing Mitigation – Prevention before breaches; any breaches will be responded to

use or disclose it for personal purposes				system will be in locked rooms.		immediately following University procedure.
Unauthorized individuals at Cloudbeds could access PI	Low	High	Med	Employees of Cloudbeds are required to act in a manner consistent with their privacy policy and client agreement. Furthermore, they will not have access to CapU PI without consent and monitoring of program area administrators.	Cloudbeds staff, CapU Student Residences Staff	Ongoing Mitigation – Prevention before breaches; any breaches will be responded to immediately following Cloudbeds and then University procedure.
Privacy breach of Cloud Storage	Low	High	Med	AWS to inform Cloudbeds immediately, then Cloudbeds would inform CapU. Initiate breach response procedure from AWS, Cloudbeds, and CapU.	AWS staff, Cloudbeds staff, CapU staff	Immediately after breach is found

G. PERSONAL INFORMATION BANKS & INFORMATION SHARING AGREEMENTS

To be completed by the Privacy Officer:

1. Personal Information Bank (PIB)

PIB is a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol, or other particular assigned only to that individual. A personal information bank can be a simple list of personal information. Personal information banks contain personal information that is:

- *Linked to an identifiable individual*
- *Organized and capable of being retrieved by a personal identifier*
- *Normally compiled for a single purpose*

	YES	NO
Will this initiative result in the creation of a personal information bank?	☐	☒

If "yes", fill in the table below:

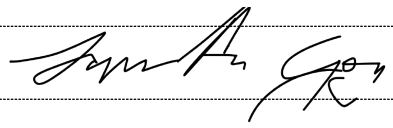
Describe the type of information in the bank:	[To be completed by the Privacy Officer] N/A
List any other ministries, agencies, public bodies, or organizations involved:	[To be completed by the Privacy Officer] N/A

Record the Business contact title and phone number for person responsible for managing the PIB:	[To be completed by the Privacy Officer] N/A

To be completed by the Privacy Officer:		
2. Information Sharing Agreements (ISAs) & Systematic or Repetitious Disclosure/Exchanges *Public bodies enter Information Sharing Agreements (ISAs) when there is a regular and systematic exchange of personal information between public sector organizations or between a public sector organization and an external agency. ISAs document the terms and conditions of the exchange of personal information in compliance with the provisions of the Act and any other applicable legislation. ISAs help to ensure privacy protection where personal information is exchanged.*		
	YES	**NO**
Does this initiative involve an Information Sharing Agreement?	☐	☒
Is the ISA added as an appendix to this PIA?	☐	☒

To be completed by the Privacy Officer:		
	YES	**NO**
Does the initiative involve a regular and systematic exchange of personal information on a regular or ongoing basis between public bodies and/or external agency(ies)?	☐	☒
If "yes", please explain. *For example: the initiative will involve systematic collection and disclosure of personal information, in order for the department to provide specific services to students.*		
[To be completed by the Privacy Officer] N/A		

H. SIGNATURES	
Project Manager Signature:	
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.	
Title:	**Director, Student Housing and Food Services**
Name:	**John Umunna**
Date:	April 10, 2025
Signature:	JU

Privacy Officer Comments & Signature:	
Comments:	All concerns have been addressed. PIA approved
Title:	**Director, Risk Management and Privacy Officer**
Name:	**Jacquetta Goy**
Date:	April 10, 2025
Signature:	

Additional Signatures (if required):	
Comments:	Cloudbeds Conference Management System, as well as Capilano University's Student Housing Department have sufficient knowledge, practices, and mitigation strategies to protect personal information collected, used, and/or stored through this initiative. In the event of any significant changes regarding personal information are made to the Cloudbeds platform or University practices, additional privacy assessment will be done at that time.
Title:	Privacy, Freedom of Information, and Records Management Coordinator
Name:	Isabel Melendez
Date:	9-Apr-2025
Signature:	Isabel Melendez

I. APPENDICES		
	YES	NO
Will this PIA include appendices?	☒	☐
If "yes", please list them, and combine them with the PDF of this PIA. *For example: excerpt from a contract/privacy schedule, third party provider policies, blank questionnaire/examples of PI being collected during the course of the initiative.*		
The Cloudbeds Terms of Service and Privacy Policy are appendices to this PIA		

CLOUDBEDS PRIVACY POLICY

Updated September March 25, 2025

You may access the previous version of our Privacy Policy containing our California Privacy Notice and EU Privacy Policy here.

This Privacy Policy describes the privacy practices of Digital Arbitrage, Inc. d/b/a Cloudbeds and its affiliated companies (“Cloudbeds”, "we", "us" and/or "our"), for data and personal information we collect:

- Through websites owned and operated by us, including https://www.cloudbeds.com/ and other websites owned or controlled by Cloudbeds (“Sites”);
- Through software applications (including chat functionality and other automated tools) made available by us for use through computers and mobile devices (“Apps”);
- Through social media pages that we control from which you are accessing this Privacy Policy (“Social Media Pages”);
- Through communications that we send to you that link to this Privacy Policy and through your communications with us online or in person;
- From other third party sources such as public databases, marketing partners, etc.

In this Privacy Policy we refer to the Sites, Apps, Social Media Pages and Offline Interactions as the “Services”.

Please note that this Privacy Policy does not apply to our processing of personal information on behalf of and subject to the instructions of third parties such as airlines, car rental companies and other service providers, companies that organize or offer packaged travel arrangements, marketing partners, or certain corporate customers.

Travelers please note, if you are booking stays or travel services with a travel provider, Cloudbeds may provide the platform through which such actions occur. **However**, your interactions, including any personal information that you share with a travel provider, are subject to the privacy policies of each such travel provider.

California Notice at Collection/State Privacy Rights Notice: See the State Privacy Rights Notice section below for important information about your rights under applicable state privacy laws.

Notice to European users: If you are located in the European Economic Area (“EEA”) or the United Kingdom (“UK”) (referred to below as “Europe” and “European”), see the Notice to European users below.

Cloudbeds may provide additional or supplemental privacy policies to individuals for specific products or services that offer at the time we collect personal information. For example, this Privacy Policy does not apply to personal information that we collect about from Cloudbeds employees, partners, contractors or job candidates. Such information is subject to separate privacy policies.

You can download a printable copy of this Privacy Policy.

INDEX

Personal information we collect

INFORMATION YOU PROVIDE TO US

We receive and store any personal information you post to the Sites or provide to us when you set up a user account, sign up for our newsletters or promotions, purchase services, or make a reservation for travel services through one of our Services. You can choose not to provide such personal information, in which case you will not be able to access or use portions of the Sites or some of their features.

- **Contact data**, such as your first and last name, salutation, billing and mailing addresses, phone number, email address, professional title, and company name.
- **Demographic data**, such as your city, state, country of residence, and postal code.
- **Communications data**, including details from our interactions with you via various channels such as:
  - **Electronic Communications:** Information from emails, online chats, and messages you send through our Services.
  - **SMS/Text Messages:** If you opt into our SMS/MMS messaging programs, we will collect and use your mobile phone number to send messages as described in our SMS/MMS Terms. Additionally, we also collect content and metadata (e.g., date, time) of text messages you send to or receive from us.
  - **Phone Calls:** Details from phone conversations with our representatives, which may include call duration, time, and, where permitted by law, recorded content.

    - **Support:** Screenshots, videos, or other information you provide to our support team to assist with inquiries or investigations.
- **User-Generated Content (UGC)**, including photographs, videos, reviews, and other content you upload or share through our Services or on social media platforms that we access, including any metadata associated with such content.
- **Online identifiers and account information**, such as your username or passwords for any of our websites.
- **Payment and transactional data**, including payment card information or bank account numbers used to bill for our services and your billing and payment history.
- .
- **Marketing data**, such as your preferences for receiving our marketing communications and details about your engagement with them.
- **Audio, electronic, and visual information**, such as video and voice recordings of conversations with you as permitted by law.
- **Professional or employment-related information**, such as your job title, employer information, work history and education information, such as the schools you attended.
- **Other data not specifically listed here**, which we will use as described in this Privacy Policy or as otherwise disclosed at the time of collection.

THIRD PARTY SOURCES

We may combine personal information we receive from you with personal information we obtain from other sources, such as:

- **Public sources**, such as government agencies, public records, social media platforms, and other publicly available sources.
- **Private sources**, such as data providers, social media platforms, data licensors, account intelligence providers (who help us identify the types of visitors to our Services), and entities to which we provide services (which may include your employer).
- **Partner organizations**, such as the travel and accommodations providers with whom we work.
- **Marketing partners**, such as joint marketing partners and event co-sponsors.

AUTOMATED COLLECTION

We, our service providers and our business partners may automatically receive and store certain types of information about you, your computer or mobile device, and you interaction with our Services over time, our communications and other online services such as:

- **Log data** - Our web servers may collect "log data." Log data provides aggregate information about the number of visits to different pages on the Sites. Third-party vendors may also collect aggregate log data independently from us.
- **Web beacons** - Some of the pages on the Sites may contain electronic images known as web beacons that allow use to count the number of users who have visited those pages. These collect only limited information such as a cookie number, time and date of a page view, and a description of the page on which the web beacon resides. These web beacons do not carry any personal information and you cannot opt-out or refuse them. However, where they operate with cookies, you can render them ineffective by opting out of cookies or changing the cookie setting in your browser.
- **Communication interaction data** such as your interactions with our email (sent by us, and/or our marketing service providers), chat messages, voicemail, text or other communications (e.g., whether you open and/or forward emails) – we may do this through use of pixel tags (which are also known as clear GIFs), which may be embedded invisibly in our emails.

(collectively, "Device Data")

COOKIES

Some of our automatic data collection is facilitated by cookies and similar technologies. For more information, see our Cookie Policy.

DETAILS ABOUT OTHERS

We may collect contact details about individuals whom you refer to us for services. Please do not refer someone to us or share their contact details with us unless you have their permission to do so.

SENSITIVE DATA

Except for biometric data (see below), we do not collect sensitive data, for example, health data, or data revealing racial or ethnic origin, from visitors to the Sites.

BIOMETRIC DATA

Solely if you expressly opt-in, we may collect biometric information, such as facial recognition data or fingerprints to enhance the security of your account through Multi-Factor Authentication (MFA). This information will be used solely for identity verification purposes and will not be shared with third parties except as necessary to provide our services or as required by law. We retain biometric data only as long as needed for authentication purposes and will delete it securely in accordance with our data retention policy. By enrolling in MFA, you consent to the collection and use of your biometric information as described herein.

How we use your personal information

We are fully committed to providing you with information about the collection and use of Personal information furnished by, or collected from, those using the Services. It is our practice not to ask you for Personal information unless we need it or intend to use it. The purposes for collecting your Personal information are as follows:

Services and Operations, including:

- Communicate with you about the Services;
- Provide customer service and support;
- Process payments, including conducting authentication;
- Notify you of changes to our Services;
- Send you information you have requested;
- Process entries to a competition or promotion;
- Carry out obligations under any contract we have with you;
- In connection with the creation and maintenance of your user account;
- In connection with the processing, fulfillment, and shipment of any products or services you purchase;
- Administer membership and activity in rewards programs;
- Process transactions with partners;
- Tailor your user experience on the Sites; and
- Perform functions as otherwise described to you at the time of collection.

UGC

When you submit content to our platform, such as comments, reviews, or media files, please be aware that this information may be publicly accessible. We may share your UGC with other users, display it on our website, or distribute it through various media channels. By providing this content, you consent to its public dissemination and acknowledge that it may be viewed by others.

Research and Development

We may use your personal information for research and development purposes, including to analyze and improve the Services and our business and to develop new products and services. As part of these activities, we may create aggregated, de-identified and/or anonymized data from personal information we collect. We make personal information into de-identified or anonymized data by removing information that makes the data personally identifiable to you. We may use this aggregated, de-identified or otherwise anonymized data and share it with third parties for our lawful business purposes, including to analyze and improve the Services and promote our business and will not attempt to reidentify any such data.

Marketing

- Communicate with you by email, regular mail, telephone, or mobile devices, about products or services that may be of interest to you either from us or from other third parties;
- Develop and deliver our newsletter;
  Develop and display third-party content and advertising tailored to your interests on the Sites;

You may opt-out of our marketing communications as described in the Opt out of communications section below.

Service Improvement and Analytics

We may use your personal information to analyze your usage of the Services, improve the Services, improve the rest of our business, help us understand user activity on the Services, including which pages are most and least visited and how visitors move around the Services, as well as user interactions with our emails, and to develop new products and services.

Legal Compliance and Protection

- Comply with applicable laws, lawful requests, and legal process, such as to respond to subpoenas, investigations or requests from, or cooperate with government authorities;
- Protect our, your or others' rights, privacy, safety or property (including by making and defending legal claims);
- Audit our internal processes for compliance with legal and contractual requirements or our internal policies;
- Enforce the terms and conditions that govern the Services; and
- Prevent, identify, investigate and deter fraudulent, harmful, unauthorized, unethical or illegal activity, including cyberattacks and identity theft.

New Purposes

We may use your personal information for reasons not described in this Privacy Policy where permitted by law and when the reason is compatible with the purpose for which we collected it.

Retention

We generally store/retain your personal information as long as reasonably necessary to fulfill the purposes described in this Privacy Policy, as we determine is necessary for business records, and as required under applicable law. To determine the appropriate retention period for personal information, we may consider factors such as the amount, nature, and sensitivity of the personal information, the potential risk of harm from unauthorized use or disclosure of your personal information, the purposes for which we process your personal information and whether we can achieve those purposes through other means, and the applicable legal requirements. In some cases, we may specifically ask you for your consent to collect, use or share your personal information, such as where required by law.

When we no longer require the personal information we have collected about you, we may either delete it or de-identify, aggregate or anonymize it. If we de-identify, aggregate or anonymize your personal

information (so that it can no longer be associated with you), we may use this information indefinitely without further notice to you.

How we share your personal information

OUR PRACTICES

As a general practice, however, we do not sell, rent, or provide your Personal information to unaffiliated third parties. We may share your Personal information with the following parties and as otherwise stated in this Privacy Policy, in other applicable notices, or at the time of collection:

- **Affiliates**. Cloudbeds' affiliates.
- **Service Providers**. The third parties that provide services on our behalf or help us operate the Services, or our business (such as information technology and software services, mailing services, marketing services, event management services, and cyber and physical security services).
- **Third Parties You Designate.** Third parties where you have instructed us or provided your consent to do so (for example travel or accommodations providers with whom you are booking or otherwise transacting business). We will share personal information that is needed for these other companies to provide the services that you have requested.
- **Other Third Parties.** Third parties, such as social sites (including Facebook and Instagram), to which you subscribe in order for you to link to them through our site and view our content through those sites.
- **Business and Marketing Co-Sponsors.** Third parties with whom we co-sponsor marketing or promotions.
- **Legal Compliance.** As we believe is necessary to comply with applicable laws, statutes, or regulations, and/or to enforce this Privacy Policy and the Terms and to protect our rights and the rights of others. And as required by a court or government agency or to respond to a claim by you or a third party.
  Assignment/Corporate Change. As part of a transfer of our assets, for example in the event of a merger, acquisition, corporate change or, in the unlikely event of a bankruptcy, involving Cloudbeds.

Other Privacy Policies

Any third parties to whom we may disclose personal information may have their own privacy policies that describe how they use and disclose personal information. Those policies will govern use, handling, and disclosure of personal information once we have shared it with those third parties as described in this Policy. If you want to learn more about their privacy practices, we encourage you to visit the websites of those third parties.

Your choices with respect to your personal information

In this section, we describe the rights and choices available to all users. If you are a resident of a state that provides additional rights (e.g., California and Virginia), you may find additional information about your rights in the State Privacy Rights Notice section below. If you are located in the EEA or the UK, see the European Privacy Rights Notice section below.

- **Opt-out of communications.** You may opt-out of marketing-related emails by following the opt-out or unsubscribe instructions at the bottom of the email. You may opt-out of marketing-related texts by texting STOP in response to a marketing text from us. Please note that if you choose to opt-out of marketing-related emails and/or texts, you may continue to receive service-related and other non-marketing emails and/or texts.
- **Cookies.** For information about cookies employed by the Services and how to control them, see our Cookie Notice.
- **Do Not Track.** Some Internet browsers may be configured to send "Do Not Track" signals to the online services that you visit. We currently do not respond to "Do Not Track" signals. To find out more about "Do Not Track," please visit http://www.allaboutdnt.com.
- **Blogs.** The Site may offer publicly accessible blogs and social forums where you may post photos, videos and information about yourself and your experience at the Properties. You should be aware that any information you provide in these areas may be read, collected, and used by others who access them. To request removal of your personal information from our blog or social pages, contact us at privacy@Cloudbeds.com. In some cases, we may not be able to remove your personal information, in which case we will let you know if we are unable to do so and why. Alternatively, if you used a third party application to post such information, you can remove it by logging into that application and removing the information, or by contacting the appropriate party for such third party application.
- **Testimonials.** We display personal testimonials of satisfied customers on our site in addition to other endorsements. With your consent we may post your testimonial along with your name. If you wish to update or delete your testimonial, you can contact us at privacy@Cloudbeds.com.
- **Storage.** If you would like us to delete the personal information you have provided to us, please contact us at privacy@Cloudbeds.com and we will respond in a reasonable time. Please note that some or all of this information may be required in order for you to make use of services and features available via the Sites. If you remove this information, you may no longer be able to use these features.
  Declining to provide information. We need to collect personal information to provide certain services. If you do not provide the information we identify as required or mandatory, we may not be able to provide those services.

Security Safeguards

We have reasonable security measures in place to protect against loss, misuse and alteration of personal information under our control. When you enter personal information to book a reservation or set up an account, we encrypt that information using secure socket layer technology (SSL). In addition, electronically stored personal information is stored and backed-up on a secure network with firewall protection and access to our electronic information systems requires user authentication via password or similar means. We also employ access restrictions, limiting the scope of employees who have access to personal information. While we strive to safeguard personal information, we cannot guarantee or warrant the security of any information you disclose or transmit to us and you do so at your own risk.

Third Party Sites

The Sites may contain links to other websites. We do not control, and make no representations whatsoever regarding, such other websites or the products and services offered by or through websites accessed through links on the Sites, even those with which we may have an affiliation. If you decide to access third party websites linked through the Sites you do so at your own risk. You should carefully review the Privacy Policy and terms of these websites.

International data transfers

We are headquartered in the United States and may use service providers that operate in other countries. Your personal information may be transferred to the United States or other locations where privacy laws may not be as protective as those in your state, province, or country.
If you are located in the EEA or the UK, see the European Privacy Rights Notice below.

Children

The Services are not directed at children, and we do not knowingly collect personal information directly from users under the age of 13 or from other websites or services directed at children. Consistent with the Federal Children's Online Privacy Protection Act of 1998 (COPPA), we will not knowingly request or collect personal information from any child under age 13 without obtaining the required parental consent.

Changes to this Privacy Policy

We reserve the right to modify this Privacy Policy at any time. If we make material changes to this Privacy Policy, we will notify you by updating the date of this Privacy Policy and posting it on the Site or other appropriate means. Any modifications to this Privacy Policy will be effective upon our posting the modified version (or as otherwise indicated at the time of posting). In all cases, your use of the Services after the effective date of any modified Privacy Policy indicates your acknowledging that the modified content of the Privacy Policy applies to your interactions with the Services and our business.

How to contact us

If you have questions or concerns regarding this Privacy Policy or our processing of personal information, you may contact us as follows:

- Complete and submit this form
- Regular Mail:

Digital Arbitrage, Inc.
3033 Fifth Ave Ste 100
San Diego, CA 92103

STATE PRIVACY RIGHTS NOTICE

This section provides additional information to individuals in states with privacy laws that provide additional rights to their residents, including the California Consumer Privacy Act ("**CCPA**"), the Virginia Consumer Data Protection Act ("**CDPA**"), the Colorado Privacy Act ("**CPA**"), and the Connecticut Personal Data Privacy and Online Monitoring Act (collectively the "**State Privacy Laws**").

This section describes how we collect, use, and share Personal information (as defined below) of residents of these states and the rights these users may have with respect to their Personal information. Please note that not all rights listed below may be afforded to all users and that if you are not a resident of one of these states with State Privacy Laws, you may not be able to exercise these rights. In addition, **we may not be able to process your request if you do not provide us with sufficient detail to allow us to confirm your identity or understand and respond to it.**

For purposes of this section, the term "**Personal Information**" has the meaning given to "personal data," "personal information" or other similar terms in applicable State Privacy Laws and does not include information exempted from the scope of the State Privacy Laws, such as publicly available information. In some cases, we may provide a different privacy policy to certain categories of residents of these states, such as job applicants, in which case that notice will apply instead of this section. "**Sensitive**

Your privacy rights. The State Privacy Laws may provide residents with some or all of the rights listed below. However, these rights are not absolute and some State Privacy Laws do not provide these rights to their residents. Therefore, we may decline your request in certain cases as permitted by law. We do not "sell" or "share" Personal information as those terms are defined in applicable State Privacy Laws (and have not done so during the prior 12 months) and have no actual knowledge that we have sold or shared the Personal information of children under 16 years of age. We do not engage in any "Profiling" (as such term is defined under applicable State Privacy Laws) in furtherance of decisions that produce legal or similarly significant effects about you, where regulated by applicable State Privacy Laws. We also do not use or disclose Sensitive Personal information for purposes that California residents have a right to limit under the CCPA, and where required by applicable State Privacy Laws, we obtain your consent before we collect Sensitive Personal information from you.

DISCLOSURE OF PERSONAL INFORMATION WE COLLECT ABOUT YOU

You have the right to know:

- The categories of personal information we have collected about you;
- The categories of sources from which the personal information is collected;
- Our business or commercial purpose for collecting or selling personal information;
- The categories of third parties with whom we share personal information, if any; and
- The specific pieces of personal information we have collected about you.

Please note that we are not required to:

- Retain any personal information about you that was collected for a single one-time transaction if, in the ordinary course of business, that information about you is not retained;
- Reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information; or
- Provide the personal information to you more than twice in a 12-month period.

PERSONAL INFORMATION SOLD OR USED FOR A BUSINESS PURPOSE

In connection with any personal information we may sell or disclose to a third party for a business purpose, you have the right to know:

- The categories of personal information about you that we sold and the categories of third parties to whom the personal information was sold; and
- The categories of personal information that we disclosed about you for a business purpose.

You have the right under the CCPA and certain other privacy and data protection laws, as applicable, to opt-out of the sale of your personal information. If you exercise your right to opt-out of such sale of your personal information, we will refrain from selling your personal information unless you subsequently provide express authorization for the sale of your personal information. To opt-out of the sale of your personal information, visit our homepage and click on the Do Not Sell My personal information link in the footer.

RIGHT TO DELETION

Subject to certain exceptions set out below, on receipt of a verifiable request from you, we will:

- Delete your personal information from our records; and
- Direct any service providers to delete your personal information from their records.

Please note that we may not delete your personal information if it is necessary to:

- Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by you, or reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform a contract between you and us;
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity;
- Debug to identify and repair errors that impair existing intended functionality;
- Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law;
- Comply with the California Electronic Communications Privacy Act;
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when our deletion of the information is likely to render impossible or seriously impair the achievement of such research, provided we have obtained your informed consent;
- Enable solely internal uses that are reasonably aligned with your expectations based on your relationship with us;
- Comply with an existing legal obligation; or
- Otherwise use your personal information, internally, in a lawful manner that is compatible with the context in which you provided the information.

PROTECTION AGAINST DISCRIMINATION

You have the right to not be discriminated against by us because you exercised any of your rights under the CCPA or other state laws. This means we cannot, among other things:

- Deny goods or services to you;

- Charge different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties;
- Provide a different level or quality of goods or services to you; or
- Suggest that you will receive a different price or rate for goods or services or a different level or quality of goods or services.

Please note that we may charge a different price or rate or provide a different level or quality of goods and/or services to you, if that difference is reasonably related to the value provided to our business by your personal information.

EXERCISING YOUR RIGHT TO KNOW, ACCESS, APPEAL, CORRECT AND DELETE PERSONAL INFORMATION

You may submit requests to exercise your right to information/know, access, appeal, correction, or deletion by calling us at +1 at (858) 345-5316 (toll-free in the U.S. only) or by completing our online data subject request form available at https://xxxxxxxx.com.

VERIFICATION OF IDENTITY; AUTHORIZED AGENTS

We may need to verify your identity in order to process your information/know, access, appeal, correction, or deletion requests and reserve the right to confirm your residency. To verify your identity, we may require government identification, a declaration under penalty of perjury, or other information, where permitted by law.

Under some State Privacy Laws, you may enable an authorized agent to make a request on your behalf. However, we may need to verify your authorized agent's identity and authority to act on your behalf. We may require a copy of a valid power of attorney given to your authorized agent pursuant to applicable law. If you have not provided your agent with such a power of attorney, we may ask you to take additional steps permitted by law to verify that your request is authorized, such as by providing your agent with written and signed permission to exercise your State Privacy Laws rights on your behalf, the information we request to verify your identity, and confirmation that you have given the authorized agent permission to submit the request.

CATEGORIES OF PERSONAL INFORMATION WE COLLECT USE AND DISCLOSE

We have summarized the Personal Information we collect and may disclose to third parties by reference below to both (i) the categories defined in the Personal information We Collect section of this Privacy Policy above and (ii) the categories of Personal information specified in the CCPA (Cal. Civ. Code §1798.140). We may use each of the categories of Personal information below for the purposes identified in the How We Use Your Personal information section of this Privacy Policy above (except for any Sensitive Personal information, which will only be processed for the purposes for which it was collected and as otherwise specifically permitted by applicable law, including applicable State Privacy Laws). This section also describes our practices currently and during the 12 months preceding the effective date of this Privacy Policy. Information you voluntarily provide to us, such as in free-form webforms, may contain other categories of Personal information not described below. More information about the categories of sources from which we collect Personal information and the purposes for collecting or disclosing Personal information are described above in this Privacy Policy.

Personal information ("PI") we collect	CCPA Statutory Category	Categories of third parties to whom we "disclose" PI for a business purpose
● Contact data	● Identifiers ● Commercial information ● California customer records	● Affiliates ● Service providers ● Third parties designated by you ● Professional advisors ● Authorities and others ● Business transferees ● Business and marketing co-sponsors
● Demographic data	● Identifiers ● California customer records	● Affiliates ● Service providers ● Third parties designated by you ● Professional advisors ● Authorities and others ● Business transferees ● Business and marketing co-sponsors
● Online identifiers and account information	● Identifiers	● Affiliates ● Service providers ● Third parties designated by you ● Professional advisors ● Authorities and others ● Business transferees ● Business and marketing co-sponsors
● Communications data	● Identifiers ● Commercial information ● California consumer records ● Internet or Network Information	● Affiliates ● Service providers ● Third parties designated by you ● Professional advisors ● Authorities and others ● Business transferees ● Business and marketing co-sponsors
● Payment and transactional data	● Commercial information ● California consumer records	● Affiliates ● Service providers

	● Financial information	● Third parties designated by you ● Professional advisors ● Authorities and others ● Business transferees ● Business and marketing co-sponsors
● Marketing data	● Identifiers ● Commercial information ● California customer records ● Internet or Network Information	● Affiliates ● Service providers ● Third parties designated by you ● Professional advisors ● Authorities and others ● Business transferees ● Business and marketing co-sponsors
● Dietary information	● Identifiers ● Commercial information ● California customer records	● Affiliates ● Service providers ● Third parties designated by you ● Professional advisors ● Authorities and others ● Business transferees ● Business and marketing co-sponsors
● Audio, electronic, and visual information	● Audio information (e.g., recordings of phone calls) ● Visual information (UGC photos/videos, videos of online meetings/calls) ● Biometric data (facial recognition data, fingerprints) ● California customer records	● Affiliates ● Service providers ● Third parties designated by you ● Professional advisors ● Authorities and others ● Business transferees ● Business and marketing co-sponsors
● Data about others	● Identifiers ● California customer records	● Affiliates ● Service providers ● Third parties designated by you ● Professional advisors ● Authorities and others ● Business transferees

		• Business and marketing co-sponsors
• Device data	• Identifiers • Internet or Network Information	• Affiliates • Service providers • Third parties designated by you • Professional advisors • Authorities and others • Business transferees • Business and marketing co-sponsors
• Online activity data	• Identifiers • Commercial information • Internet or Network information	• Affiliates • Service providers • Third parties designated by you • Professional advisors • Authorities and others • Business transferees • Business and marketing co-sponsors
• General location data	• Geolocation data	• Affiliates • Service providers • Third parties designated by you • Professional advisors • Authorities and others • Business transferees • Business and marketing co-sponsors
• Communication interaction data	• Identifiers • Commercial information • Customer records information • Internet or Network Information	• Affiliates • Service providers • Third parties designated by you • Professional advisors • Authorities and others • Business transferees • Business and marketing co-sponsors
• Data derived from the above	• Inferences	• Affiliates • Service providers

		● Third parties designated by you ● Professional advisors ● Authorities and others ● Business transferees ● Business and marketing co-sponsors
● Purchase history	● Identifiers ● California customer records ● Commercial information	● Affiliates ● Service providers ● Third parties designated by you ● Professional advisors ● Authorities and others ● Business transferees ● Business and marketing co-sponsors
● Professional or employment related information	● Identifiers ● California customer records	● Affiliates ● Service providers ● Third parties designated by you ● Professional advisors ● Authorities and others ● Business transferees ● Business and marketing co-sponsors

Any request for a disclosure required under this California law should be sent to us via email at support@cloudbeds.com or via regular mail at:

Digital Arbitrage, Inc.
3033 Fifth Ave Ste 100
San Diego, CA 92103

Please note that under this law, we are not required to respond to your request more than once in a calendar year, nor are we required to respond to any request that is not sent to the email or mailing address designated above.

“Do not track": Section 22575 of the California Business & Professions Code requires website and online service operators to disclose whether they honor web browser “Do Not Track” settings. We support and honor “Do Not Track” web browser settings. If you enable Do Not Track settings in the browser you are using, we will not collect, store, or use personal information about websites you visit using that browser other than privacy@Cloudbeds.com and our other Sites. Other parties, however, may not honor Do Not

Track signals. These parties may collect personal information about your online activities over time and across different web sites when you visit the Sites, for example by using cookies on our Sites. We have no access to or control over other parties' personal information collection practices, even those with which we may have an affiliation. You should carefully review the Privacy Policy and terms of any website you visit. For more information about Do Not Track, please visit www.allaboutdnt.org.

Nevada privacy rights

Chapter 603A of the Nevada Revised Statutes permits a Nevada resident to opt out of future sales of certain covered information that a website operator has collected or will collect about the resident. If you are a Nevada resident, you may submit a request to opt out of potential future sales under Nevada law by contacting us as indicate below. Please include sufficient information for us to identify you in your email, such as information about stays, or, if applicable, your account information. Please note we will take reasonable steps to verify your identity and the authenticity of the request.

EUROPEAN PRIVACY RIGHTS NOTICE

The Sites are hosted in and provided from the United States. If you use the Sites from the European Union, Canada, or other regions with laws governing data collection and use that may differ from U.S. law, please note that you are transferring your personal information to the United States for storage and processing. The United States does not have the same data protection laws as the EU, Canada, and some other regions. Also, we may transfer your data from the United States to other countries or regions in connection with storage and processing of data, fulfilling your requests, and operating our business. By providing any information, including personal information, you consent to the transfer of that information to the United States and the use of your personal information, in accordance with this Policy.

The information provided in this "Notice to European users" section applies only to individuals in the United Kingdom ("**UK**") and the European Economic Area ("**EEA**") (hereafter collectively referred to as "**Europe**" as defined at the top of this Privacy Policy).

Personal information. References to "personal information" in this Privacy Policy are equivalent to "personal data" governed by European data protection legislation – *i.e.,* any information relating to an identified or identifiable natural person. It does not include "anonymous data" (*i.e.,* information where the identity of individual has been permanently removed).

Controller. Cloudbeds is responsible for your personal data. Cloudbeds is a corporation formed under the laws of the State of Delaware, United States of America. For the purposes of European data protection legislation, your data will be controlled by Cloudbeds.

Data Protection Officer. Our data protection officer can be contacted at: privacy@cloudbeds.com or at the following postal address: 3033 Fifth Ave #100, San Diego, California 92103.

Legal bases for processing. In respect of each of the purposes for which we use your personal information, the European data protection legislation requires us to ensure that we have a legal base for that use. The legal bases of our processing of your personal information as described in this Privacy Policy will depend on the type of personal information and the specific context in which we process it. However, the legal bases we typically rely on are set out in the table below. If you have questions about the legal basis of how we process your personal information, contact us at privacy@cloudbeds.com:

Processing purpose *Details regarding each processing purpose listed below are provided in the section above titled "How we use your personal information."*	Categories of personal information involved *Details regarding the categories of personal information listed below are provided in the section above titled "Personal information we collect."*	Legal basis
1. Service delivery and operations: We need to process your personal information to operate the Services, including responding to your requests or inquiries, providing you with access to content or information you requested, etc.	• Contact data • Demographic data • Communications data • Online identifiers and account information • Payment and transactional data • Marketing data • Audio, electronic, and visual information • Internet activity or electronic network activity information • Other data • Device Data	Processing is necessary to perform the contract governing our provision of our Services or to take steps that you request prior to signing up for the Services. We also process this information where we have collected your consent.
2. For research and development: We may use your personal information for research and development purposes, including to analyze and improve the Service and our business.	Any and all data types relevant in the circumstances	These activities constitute our legitimate interests. We do not use your personal information for these activities where our interests are overridden by the impact on you.
3. We may need to process your personal information for additional purposes, such as: • To ensure access and maintenance of the Services, and to ensure their proper functioning. • For compliance, fraud prevention and safety. • For sharing your personal information with third parties as described in this Privacy Policy.	• Contact data • Demographic data • Communications data • Online identifiers and account information • Payment and transactional data • Marketing data • Audio, electronic, and visual information • Internet activity or electronic network activity information • Other data • Device Data	We rely on our legitimate interests to process your personal information when performing these processing activities. We do not use your personal information for these purposes where our interests are overridden by the impact on you.

● To disclose your personal information to a prospective or actual purchaser or seller in the context of a merger, acquisition or other reorganization or sale of our business or assets. ● For the collection of statistical information about the use of the Services. ● To protect our interests as a company, for different purposes, such as: ● Enforcement of the Terms of Service. ● Assess claims that any content violates the rights of third-parties. ● For the establishment or exercise our legal rights or defending against legal claims.		
4. For marketing and advertising purposes: We and our third-party advertising partners may collect and use your personal information for marketing and advertising purposes.	● Contact data ● Demographic data ● Communications data ● Device data ● Internet activity or electronic network activity information ● Marketing data ● Other data	Processing is based on your consent where that consent is required by applicable law. Where such consent is not required by applicable law, we process your personal information for these purposes based on our legitimate interests in promoting our business.
5. Compliance with legal obligations and protection purposes: We are subject to certain legal obligations that may oblige us to disclose your personal information to courts, law enforcement or regulatory authorities.	Any and all data types relevant in the circumstances.	Processing is necessary to comply with our legal obligations. Where Compliance with Law is not applicable, we and any relevant third parties have a legitimate interest in participating in, supporting, and following legal process and requests, including through co-operation with authorities. We and any relevant third parties may also have a

		legitimate interest of ensuring the protection, maintenance, and enforcement of our and their rights, property, and/or safety.
6. Further uses: We may use your personal information for reasons not described in this Privacy Policy.	Any and all data types relevant in the circumstances.	The original legal basis relied upon, if the relevant further use is compatible with the initial purpose for which the Personal information was collected. Consent, if the relevant further use is not compatible with the initial purpose for which the personal information was collected.

Your rights. Subject to certain exemptions, and in some cases dependent upon the processing activity we are undertaking, you may have the following rights under data protection laws:

1. **Right of access:** You have the right to ask us for copies of your personal information.
2. **Right to rectification:** You have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.
3. **Right to erasure:** You have the right to ask us to erase your personal information in certain circumstances.
4. **Right to restriction of processing:** You have the right to ask us to restrict the processing of your personal information in certain circumstances.
5. **Right to object to processing:** You have the right to object to the processing of your personal information in certain circumstances.
6. **Right to data portability:** You have the right to ask that we transfer the personal information you gave us to another organization, or to you, in certain circumstances.
7. **Right to withdraw consent at any time:** Where we are relying on consent to process your personal data, you have the right to withdraw your consent at any time. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent.

Exercising These Rights. You may submit these requests by email to privacy@cloudbeds.com or at the following postal address: 3033 Fifth Ave #100, San Diego, California 92103. We may request specific information from you to help us confirm your identity and process your request. Whether or not we are required to fulfill any request you make will depend on a number of factors (*e.g.,* why and how we are processing your personal information), if we reject any request you may make (whether in whole or in part) we will let you know our grounds for doing so at the time, subject to any legal restrictions.

Your Right to Lodge a Complaint with Your Supervisory Authority. In addition to your rights outlined above, if you are not satisfied with our response to a request you make, or how we process your personal information, you can make a complaint to the data protection regulator in your habitual place of residence.

- For users in the European Economic Area – the contact information for the data protection regulator in your place of residence can be found here: **https://edpb.europa.eu/about-edpb/board/members_en**
- For users in the UK – the contact information for the UK data protection regulator is below:
    - The Information Commissioner's Office
    - Water Lane, Wycliffe House Wilmslow - Cheshire SK9 5AF
    - Tel. +44 303 123 1113
    - Website: **https://ico.org.uk/make-a-complaint/**

Onward transfer

Except as otherwise provided in this Privacy Policy, we only disclose personal information to third parties who reasonably need to have access to it for the purpose of the transaction or activity for which it was originally collected or to provide services to or perform tasks on our behalf or under our instruction. All such third parties must agree to use such the personal information we provide to them only the purposes for which we have engaged them and they must either: (a) comply with a mechanism permitted by the applicable EU & Swiss data protection law(s) for transfers and processing of personal information; or (b) agree to provide adequate protections for the personal information that are no less protective than those set out in this Privacy Policy. Where we have knowledge that an entity to whom we have provided personal information is using or disclosing personal information in a manner contrary to this Privacy Policy, we will take reasonable and appropriate steps to prevent, remediate or stop the use or disclosure.

You can obtain further information or a copy of or access safeguards under which your personal information is transferred outside of the EEA and/or UK by contacting us at 3033 Fifth Ave #100, San Diego, California 92103.

Profiling

We may analyze personal information we have collected about you to create a profile of your interests and preferences so that we can contact you with information that is relevant to you. We may make use of additional information about you when it is available from external sources to help us do this effectively. We may also use personal information about you to detect and reduce fraud and credit risk.

If you have questions or complaints regarding this Policy or our handling of your personal information, please contact support@cloudbeds.com. We will promptly investigate and attempt to resolve complaints and disputes in a manner that complies with the principles described in this Privacy Policy. Residents of Switzerland should contact us with questions at the same address.

Enforcement and disputes

We commit to resolve complaints about your privacy and our collection or use of your personal information. If you do not receive timely acknowledgement of your request or have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact us as set out in the "How to contact us" section above.

In addition to the above, you may complain to your home data protection authority and can invoke binding arbitration for some residual claims not resolved by other redress mechanisms. Contact details for the EU data protection authorities can be found at http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

Other terms and conditions

Your access to and use of the Sites and our Services are also subject to our Terms.

Effective March 2025

Updated as of July 2, 2024

Terms of Service

1. ACCEPTANCE OF TERMS. Digital Arbitrage, Inc., which owns and operates www.Cloudbeds.com ("Company") and you enter into this agreement subject to the following Terms Of Service ("Terms"). The terms govern your contractual relationship with Company, including but not limited to your use of Company's website, www.Cloudbeds.com ("Website"), as well as your use of the Services (defined below). They create legally binding obligations, and you should review them carefully before accessing the Website or using any of the Services. If you are accessing the Website on behalf of a company or other entity, you represent and warrant that you are authorized to bind such entity to the provisions hereof. The Terms may be revised from time to time without notice, and the then-current version of the Terms will apply to any transaction or action or omission of you or the Company. This Agreement shall apply for an indefinite term and may be terminated by either party by providing thirty days' notice to the other party.

When you accept these Terms, you also agree to the provisions of our Privacy Policy https://www.cloudbeds.com/privacy-policy/, which is incorporated into these Terms. You agree that Company may process your personal data in the manner described in the Privacy Policy, and you agree that you will not process the personal data of any third person with whom you may come in contact through the use of the Services, except in compliance with the Privacy Policy. When you become a customer of Company, you are eligible to enter into a Data Protection Addendum ("DPA") with Company. The DPA is posted at https://myfrontdesk.cloudbeds.com/hc/en-us/articles/360004599594-Cloudbeds-Data-Processing-Agreement. It sets forth the obligations of the parties with respect to the General Data Protection Regulation ("GDPR") enacted in Europe and made enforceable beginning May 25, 2018. Adopting the DPA allows for the processing of personal data of European data subjects by companies outside the EU. You must follow the directions set forth in the DPA to make it effective between you and Company.

2. COMMUNICATIONS. When you visit the Website or send e-mails to us, you are communicating with us electronically. You consent to receive communications from us electronically. We will communicate with you by e-mail or by posting notices on the Website. You agree that all agreements, notices, disclosures and other communications that we provide to you electronically satisfy any legal requirement that such communications be in writing. Any comments, materials, or letters sent by you to Company, including, without limitation, questions, comments, suggestions, criticisms or the like ("Received Materials"), may be deemed by Company to be non-confidential and free of any claims of proprietary or personal rights. Company shall have no obligation of any kind with respect to such Received Materials and Company will be free to reproduce, use, disclose, exhibit, display, transform, edit, abridge, create derivative works from and/or distribute the Received Materials without limitation or restriction. Furthermore, Company is free to use any ideas, concepts, know-how, or techniques contained in any communication you send to Company for any purpose whatsoever, including, but not limited to, developing, manufacturing, and marketing products using such information or ideas, without compensation or any other obligations to anyone, including you. You agree that any information you receive from Company related to Company's operations, plans, customers, methods, business, finances, procedures, and other information that would reasonably be considered confidential shall be considered Confidential Information and that you will not disclose any Confidential Information to third parties during the term of this Agreement and for a period of five years after its expiration.

3. DESCRIPTION OF SERVICES AND PRODUCTS. Company provides users with a rich collection of services through the Website that allow users to manage properties in the travel industry, promote those properties, and distribute information related to availability and booking through the Website ("Services"). For purposes of clarity, the term "Services" includes all functionality made available through the Website, such as the help desk system, connectivity API's, and related support services. Any new features which augment or enhance the current Services, including the release of new features or products, is also governed by the Terms. Company reserves the right at any time to change or discontinue the Services with or without notice. You agree that Company shall not be liable to you or to any third party for any modification, suspension, or discontinuance of any of the Services. If a service or product is listed on the Website at an incorrect price or with incorrect information, we reserve the right to refuse or cancel orders placed for that service or product, whether or not the order has been confirmed and even if your account has been charged (in which event a credit will be issued to your account in the amount of the charge).Our creation or transmission of an order confirmation does not signify acceptance of your order, nor constitute a binding confirmation of an offer to sell any service offered on the Website, and we reserve the right to accept or decline your order for any reason. We may contact you and require additional information from you before we grant such approval. Services on the Website are offered for sale only to end user customers and not for resale. We reserve the right to refuse, cancel or seek the return of any services or products that are purchased in violation of our policies and restrictions. You are responsible for any taxes imposed on the sale or use of Services and applicable taxes may be added to the amount charged for Services purchased on the Website.

4. ACCESS AND FEES. You are responsible for obtaining access to the Services, which may require transacting with third parties, such as internet providers. Fees charged for the Services are as disclosed on the Website. Your use of the Website is subject to the timely payment of such fees plus all applicable taxes.

5. LICENSE AND SITE ACCESS. Company hereby grants you, subject to the Terms, a limited non-exclusive, non-sublicensable, non-transferable, license to use the Services. You may not download any portion of the Website or use of any Services other than for your own personal use. You may not use any data mining, robots, or similar data gathering tools or otherwise exploit your access to the Services for any commercial purpose. You may not use any of the trademarks, logos, or other proprietary graphics without express written permission, which may denied in Company's absolute discretion. Company's logos and product and service names are trademarks of Company. All other trademarks appearing on the Website or in connection with the Products or Services are trademarks of their respective owners, and our reference to them does not imply or indicate any approval or endorsement by their owners unless such approval or endorsement is expressly made. You may not attempt to disassemble, decompile, reverse engineer, or otherwise modify or attempt to access the software, related code, or any portion of the Services.

6. YOUR ACCOUNT. You are responsible for maintaining the confidentiality of any account information, including your login and password, and for restricting access to your computer, and you agree to accept responsibility for all activities that occur under your account or password. Company reserves the right to refuse service, terminate accounts, remove or edit content, or cancel orders in its sole discretion. You are also solely responsible for the accuracy and currency of the data entered into the Services under your user account. You agree to indemnify and hold Company harmless from and against any claim related to content, accuracy, or currency of the information you provide through the Services.

7. LINKS. Company may provide links to other websites or resources. Because Company has no control over such sites and resources, you acknowledge and agree that Company is not responsible for the availability or content of such external sites or resources. You may create a link to the Website so long as the link does not portray Company or its products or services in a false, misleading, derogatory, otherwise offensive manner. You may not use any of Company's logos, trademarks, or other proprietary graphics as part of your link. Company may refer to you certain products or services from third parties, and/or may collaborate with third parties to provide the Services to you, in which case Company may receive certain compensation from such third parties.

8. COPYRIGHT and TITLE. The Services and all copyrights, trade secrets and other proprietary rights therein, including any derivative work, are, and will remain the sole property of Company, regardless of the use made by you; and are protected by certain United States and international copyright laws and trademark laws. The Terms confer no title of ownership in the Services, other than in the products you purchase, and are not a sale of any rights in the Services, including any intellectual property rights related thereto.

9. WARRANTY. Company warrants that the Services and all elements thereof do not infringe the intellectual property rights of any third party and agree to hold you harmless and indemnify you with respect to any final judgment obtained by a third party based on a claim that the Services infringe on the intellectual property rights of such third party.

10. DISCLAIMER OF WARRANTY. EXCEPT AS EXPRESSLY SET FORTH IN SECTION 9 OF THIS AGREEMENT, THE SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE" WITHOUT WARRANTY OF ANY KIND, ORAL, WRITTEN, STATUTORY, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF PERFORMANCE OR MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Company does not warrant or guarantee the availability, accuracy, or truthfulness of any information provided by or with respect to a hotelier or other provider of services accessed through the Services, including information leading to overbooking, and you agree to hold company from and against any such claims. WITHOUT LIMITING THE FOREGOING, COMPANY DOES NOT WARRANT THAT ALL ERRORS CAN BE CORRECTED, OR THAT OPERATION OF THE WEBSITE AND/OR DELIVERY OF THE SERVICES SHALL BE UNINTERRUPTED OR ERROR-FREE. Because some jurisdictions may not allow the exclusion of implied warranties, such limitation may not apply in its entirety to Licensee. Any warranties made in this Agreement are for your benefit only.

11. LIMITATION ON LIABILITY. IN NO EVENT WILL COMPANY, ITS SUPPLIERS, SHAREHOLDERS, OFFICERS, EMPLOYEES OR AGENTS BE LIABLE FOR ANY LOST PROFITS, INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, INCLUDING DAMAGES ARISING OUT OF THIS AGREEMENT OR THE USE OF OR RELIANCE UPON THE SERVICES OR PRODUCTS, EVEN IF IT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. UNDER NO CIRCUMSTANCES WILL COMPANY'S TOTAL LIABILITY OF ANY KIND ARISING OUT OF OR RELATED TO THIS AGREEMENT AND USE OF THE SERVICES (INCLUDING BUT NOT LIMITED TO WARRANTY CLAIMS), REGARDLESS OF THE FORUM AND REGARDLESS OF WHETHER ANY ACTION OR CLAIM IS BASED ON CONTRACT, TORT, OR OTHERWISE, EXCEED THE AMOUNT PAID BY YOU DURING THE 12-MONTH PERIOD PRIOR TO SUCH CLAIM ARISING. THE PARTIES AGREE THAT THIS SECTION SHALL SURVIVE AND CONTINUE IN FULL FORCE AND EFFECT DESPITE ANY FAILURE OF CONSIDERATION OR OF AN EXCLUSIVE REMEDY. THE PARTIES ACKNOWLEDGE THAT THE PRICES HAVE BEEN SET AND THE AGREEMENT ENTERED INTO IN RELIANCE UPON THESE LIMITATIONS OF LIABILITY AND THAT ALL SUCH LIMITATIONS FORM AN ESSENTIAL BASIS OF THE BARGAIN BETWEEN THE PARTIES. BECAUSE SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, SUCH LIMITATIONS MAY NOT APPLY.

12. GOVERNING LAW AND JURISDICTION. This Agreement shall be governed by and construed in accordance with the laws of the State of California, without reference to the United Nations Convention on the International Sales of Goods. The Parties hereby submit to the exclusive jurisdiction of the state and federal courts located in the State of California.

13. ATTORNEY FEES. In case of an action to enforce any rights or conditions of the Terms, or appeal from said proceeding, it is mutually agreed that the losing party in such suit, action, proceeding or appeal shall pay the prevailing party's reasonable attorney fees and costs incurred.

14. ENTIRE AGREEMENT; AMENDMENT. The Terms are a binding contract and constitute the entire agreement and understanding of the parties, whether oral or written, relating to the subject matter hereof; are intended as the parties' final expression and complete and exclusive statement of the terms hereof, superseding all prior or contemporaneous agreements, representations, communications, and understandings, whether written or oral; and may be amended or modified only by an instrument in writing signed by both parties.

15. NON-WAIVER. No waiver of any provision of the Terms shall constitute a waiver of any other provision, whether or not similar, nor shall any waiver constitute a continuing waiver. Failure to enforce any provision of the Terms shall not operate as a waiver of such provision or any other provision or of the right to enforce such provision or any other provision.

16. NO THIRD-PARTY BENEFICIARIES. Nothing in the Terms, express or implied, is intended to confer on any person, other than the parties to the Terms, any right or remedy of any nature whatsoever.

17. SEVERABILITY; BINDING EFFECT. If any provision of the Terms shall be invalid or unenforceable in any respect for any reason, the validity and enforceability of any such provision in any other respect and of the remaining provisions of the terms shall not be impaired. The Terms shall be binding on and inure to the benefit of the parties and their heirs, personal representatives, successors, and assigns.

18. FORCE MAJEURE. Company will not be liable for or be considered to be in breach of or default under the Terms on account of, any delay or failure to perform as required by the Terms as a result of any cause or condition beyond Company's reasonable control.

19. DEFENSE AND INDEMNIFICATION. In addition to the other provisions of this Agreement, you agree to defend Company from any actual or threatened third party claim arising out of or based upon your use of the Services, your failure to comply with any of the provisions of the GDPR, and your breach of any of the provisions of the Terms. In addition, you agree to indemnify, defend, and hold harmless Company from and against: (a) all damages, costs, and attorneys' fees finally awarded against Company in any proceeding under this section; (b) all out-of-pocket costs (including reasonable attorneys' fees) reasonably incurred by Company in connection with the defense of such proceeding (other than when you have accepted defense of such claim); and (c) if any proceeding arising under this section is settled, any amounts to any third party agreed to by you in settlement of any such claims.

20. ACCEPTABLE USE POLICY
In addition to any other things that might constitute a misuse of the Services, you must not, and must not attempt to do the following things:

- modify, alter, tamper with, repair or otherwise create derivative works of any of the Services;
- reverse engineer, disassemble or decompile the software used to provide or access the Services, or attempt to discover or recreate the source code used to provide or access the Services, except and only to the extent that the applicable law expressly permits doing so;
  use the Services for research or benchmarking or any related endeavor with the intent of creating a competing or similar product;
- use the Services in any manner or for any purpose other than as expressly permitted by these Terms, the Privacy Policy, or any other policy, instruction or terms applicable to the Services;
- sell, lend, rent, resell, lease, sublicense or otherwise transfer any of the rights granted to you with respect to the Services to any third party;
- remove, obscure or alter any proprietary rights notice pertaining to the Services;
- access or use the Services in a way intended to improperly avoid incurring fees or exceeding usage limits or quotas;
- use the Services to: (i) engage in any unlawful or fraudulent activity or perpetrate a hoax or engage in phishing schemes or forgery or other similar falsification or manipulation of data; (ii) send unsolicited or unauthorized junk mail, spam, chain letters, pyramid schemes or any other form of duplicative or unsolicited messages, whether commercial or otherwise; (iii) advertise or promote a commercial product or service that is not available through Company; (iv) store or transmit inappropriate content, such as content: (1) containing unlawful, defamatory, threatening, pornographic, abusive, libelous or otherwise objectionable material of any kind or nature, (2) containing any material that encourages conduct that could constitute a criminal offense, or (3) that violates the intellectual property rights or rights to the publicity or privacy of others; (v) store or transmit any content that contains or is used to initiate a denial of service attack, software viruses or other harmful or deleterious computer code, files or programs such as Trojan horses, worms, time bombs, cancelbots, or spyware; or (vi) abuse, harass, stalk or otherwise violate the legal rights of a third party;
- interfere with or disrupt servers or networks used by Company to provide the Services or used by other users' to access the Services, or violate any third party regulations, policies or procedures of such servers or networks or harass or interfere with another user's full use and enjoyment of any of the Services;
- access or attempt to access Company's other accounts, computer systems or networks not covered by these Terms, through password mining or any other means;
- cause, in Company's sole discretion, inordinate burden on the Services or Company's system resources or capacity; or
- share passwords or other access information or devices or otherwise authorize any third party to access or use the Services.

21. COPYRIGHT
Company does not tolerate content that appears to infringe any copyright or other intellectual property rights or otherwise violates these Terms and will respond to notices of alleged copyright infringement that comply with the law and are properly provided to us. Such notices can be reported by contacting us at the address below. We reserve the right to delete or disable content alleged to violate these Terms and to terminate repeat infringers. Our contact information for notice of alleged copyright infringement is:
Digital Arbitrage, Inc.
3033 Fifth Ave Ste 100
San Diego, CA 92103

22. GDPR OBLIGATIONS. If you (1) are established in the European Union ("Union"), (2) offer goods or services to data subjects in the Union (whether or not they have to pay anything), or (3) monitor the behavior of any individuals that occurs in the Union, then you must comply with the provisions of the GDPR with respect to your use of the Services. Without limiting the generality of the foregoing, you must:

1. Obtain the consent of any data subject about whom you gather any personal data (as that term is defined in the GDPR using the Services, unless you have established that you are authorized to process information about such data subject under another lawful basis (such as a legitimate interest or contractual basis for processing such information). The consent you obtain must be clear and in compliance with the provisions of the GDPR;
2. Use the personal data you obtain using the Services only for the purposes for which consent is given or for other purposes allowed by the GDPR;
3. Notify us immediately if any data subject makes a complaint regarding your use of their personal data; and
4. Comply with any reasonable request we may make regarding compliance with the GDPR and cooperation with any applicable data protection authority.

23. PRICING. The pricing and packaging offered to you is contingent upon payment for the combined package amount, and if you choose to remove or downgrade any of the services, you understand and agree that the pricing and packaging that had been previously offered to you may be revised or changed based on the removal or downgrade. We reserve the right to increase or decrease your fees for the Services by providing you with thirty (30) days prior notice. To notify you of such an upcoming fee increase or decrease, we may post the revised fees on our website, or we may notify you directly in writing (email acceptable). Notwithstanding the foregoing, if you are under a Services subscription term that is longer than thirty (30) days, and if we notify you of an increase in your fees for those Services during that subscription term, the increased fees will only become effective when your subscription term ends. For example, if you are under a twelve (12) month subscription term for certain Services and we notify you of an increase in the fees for those Services in the fourth month of your subscription term, your fees will remain unchanged during the remaining eight months of your subscription term, and the increased fees will only become effective at the end of that subscription term.

24. NO REFUNDS. Your subscription to the Services goes into immediate effect once you enter your payment details into the system. You may cancel your subscription at any time by logging into the Services and selecting "Billing" from the main menu. If you cancel, you will not be billed for any additional terms if you are on month-to-month terms, and the Services will continue until the end of the current Agreement Term. Customers on contracts will be billed till the end of the term of the contract. If you cancel, you will not receive a refund for any Services already paid for. By clicking Accept, you certify that you agree to and understand this policy as well as the full Terms of Service located at www.cloudbeds.com/terms.

25. CLICKING SUBSCRIBE. By clicking "Subscribe" you agree to receive recurring informational SMS, MMS, or Email messages from Cloudbeds. Your click is your electronic signature, and you authorize us to send you text messages on your mobile phone or landline. You understand that consenting to receive SMS messages is not a condition of purchase or service. This is a standard rate subscription service available on most carriers, Msg & Data Rates May Apply. You can STOP messaging by sending STOP and get more help by sending HELP. Visit our Privacy Policy for more information at https://www.cloudbeds.com/privacy-policy/. You can also request additional information by sending an email to PRIVACY@CLOUDBEDS.COM. Service will continue until the customer cancels. Subscription may be canceled by emailing SUPPORT@CLOUDBEDS.COM. Further disclosure at Terms & Conditions and Privacy Policy.