



Privacy - Complaint Handling, Access and Correction Request and Breach Response - Procedure

1. Purpose

This Procedure outlines how UniLodge Canada receives, assesses, investigates, responds to, documents, and resolves privacy complaints, requests and privacy breaches.

This Procedure supports UniLodge Canada's Privacy & Confidentiality Policy and is intended to help ensure consistent handling of privacy complaints, requests and responses across UniLodge Canada.

2. Scope

This Procedure applies to privacy complaints or concerns involving any identifiable individual whose personal information is collected, used, disclosed, retained, corrected, or protected by UniLodge Canada.

This may include residents, applicants, guarantors, emergency contacts, visitors, employees, candidates, contractors, volunteers, client partner contacts, vendors, service providers, and other business contacts.

3. Guiding Principles

Privacy complaints must be handled in a manner that is:

Accessible: Individuals must be able to raise privacy concerns without unnecessary barriers.

Prompt: Complaints must be acknowledged and addressed within reasonable timelines.

Fair and impartial: Complaints must be reviewed by the Privacy Officer or an appropriate delegate who can assess the matter objectively.

Confidential: Complaint information must be shared only with those who need it to assess, investigate, resolve, or document the matter.

Documented: The complaint, review steps, outcome, and any corrective actions must be recorded.

Improvement focused: Where a complaint identifies a gap, UniLodge Canada will take reasonable steps to correct the issue and improve privacy practices.

4. Legislative Alignment

This Procedure is designed to support compliance with applicable Canadian privacy laws, including PIPEDA and applicable provincial private sector privacy legislation in British Columbia and Alberta.

Where laws differ, UniLodge Canada will generally follow the higher or more protective standard that reasonably applies to the situation.

5. Roles and Responsibilities

5.1 Privacy Officer

The Privacy Officer owns and oversees triages, complaints and incident; directs investigations, determined breach status and notification recommendations; consults legal counsel where appropriate; maintains complaint and breach records and approves closure.

5.2 Privacy Officer Delegate

A Privacy Officer delegate may assist with intake, fact gathering, record review, correspondence, tracking, and corrective actions under the Privacy Officer's direction.

The Privacy Officer must remain available for guidance and must approve responses to complex, sensitive, high risk, or escalated complaints.

5.3 Employees and Managers

Employees and managers who receive a privacy complaint or concern must promptly forward it to the Privacy Officer and must not attempt to investigate, resolve, dismiss, or respond to the complaint without guidance.

Employees and managers must preserve relevant records and cooperate with the Privacy Officer or delegate during the review.

5.4 Legal Counsel

Legal counsel should be consulted where the matter involves threat of litigation or legal claim, high risk matters or uncertainty about legal obligations.

6. What Is a Privacy Complaint?

A privacy complaint is a concern, challenge, or allegation that UniLodge Canada has not handled personal information in accordance with its Privacy & Confidentiality Policy or applicable privacy law.

7. Privacy Complaint vs. Privacy Inquiry vs. Privacy Breach

The Privacy Officer or delegate must classify the matter at intake.

Type of Matter	Description	Procedure to Follow
Privacy inquiry	A general question about the Privacy & Confidentiality Policy or privacy practices.	Respond directly or escalate to the Privacy Officer if more review is needed.
Privacy complaint	A concern that UniLodge Canada may not have handled personal information appropriately.	Follow this Procedure.
Access request	A request by an individual for access to their personal information.	Follow this Procedure and apply the access request timeline.
Correction request	A request to correct inaccurate or incomplete personal information.	Follow this Procedure and apply the correction request process.
Privacy breach	Loss of, unauthorized access to, or unauthorized disclosure of personal information.	Escalate immediately and follow the Privacy Breach Response Procedure or breach response process.

If a complaint may involve a privacy breach, the Privacy Officer must treat the matter as both a complaint and a potential breach until assessed.

8. Complaint Intake

Privacy complaints should be directed to:

Privacy Officer – UniLodge Canada

Email: privacy@unilodge.ca

Mail: 1400 – 18 King Street East, Toronto, Ontario, M5C 1C4

Complaints do not need to use a specific form. However, where possible, the complainant should be asked to provide:

- name and contact information;
- relationship to UniLodge Canada;
- property, unit, department, or location involved, if applicable;
- date or approximate date of the concern;
- description of the personal information involved;
- description of the concern;
- names of any UniLodge Canada employees, vendors, or third parties involved, if known;
- copies of relevant communications or documents; and
- the outcome or resolution being requested.

If the complaint is made verbally, the person receiving the complaint must document the details and forward them to the Privacy Officer as soon as possible.

9. Acknowledgement of Complaint

The Privacy Officer or delegate should acknowledge receipt of the complaint promptly, generally within five business days.

Where the complaint includes a request for access to personal information, a correction request, or a challenge to the accuracy or completeness of personal information, the acknowledgement must confirm the date the request was received for timeline tracking purposes.

10. Timelines

UniLodge Canada will respond to privacy complaints as soon as reasonably possible.

The following timelines apply:

Matter	Timeline
General privacy inquiry	As soon as reasonably possible.
Privacy complaint not involving access or correction	Generally, within 30 calendar days, where practical.
Access request under PIPEDA or Ontario operations where PIPEDA applies	Within 30 calendar days, unless a permitted extension applies.
Correction request tied to access or accuracy of personal information	Within 30 calendar days where practical, unless another applicable law permits or requires a different timeline.
Complex complaint involving multiple parties, legal review, third-party systems, or potential breach	Provide an update within 30 calendar days and continue to provide reasonable updates until resolved.

If additional time is required, the Privacy Officer or delegate must advise the complainant of the reason for the delay, the expected timing of the response, and any applicable right to complain to a privacy regulator.

11. Initial Assessment

The Privacy Officer or delegate must conduct an initial assessment to determine:

- whether the matter involves personal information;
- whose personal information is involved;
- whether the complainant is the individual concerned or has authority to act for the individual;
- whether identity verification is required;
- whether the matter involves a possible privacy breach;
- whether the matter includes an access or correction request;
- whether any third-party service provider is involved;
- whether any legal hold, litigation, insurance, regulatory, or contractual issue may be triggered;
- whether legal counsel should be consulted; and

- who should be involved in the review.

If the complaint does not involve personal information or privacy obligations, the Privacy Officer or delegate may redirect the matter to the appropriate department, such as Operations, HR, Finance, IT, or Resident Services.

12. Identity Verification and Authority to Act

Before disclosing personal information, discussing account specific details, or processing an access or correction request, UniLodge Canada must take reasonable steps to verify the identity and where applicable, their authority to act for or receive information about another individual.

Verification should be proportionate to the sensitivity of the information and may include confirming details already on file or requesting additional documentation.

UniLodge Canada must not collect more information than necessary to verify identity.

Where a request is made by a representative, family member, guarantor, emergency contact, lawyer, agent, power of attorney, executor, or other third party, the Privacy Officer or delegate must confirm that the individual has provided authorization or that another lawful basis permits the disclosure. Authorization may be confirmed through documentation already on file, a new written consent, legal authority, or another reliable method appropriate in the circumstances.

Employees must not release personal information to another individual, department, service provider, institutional partner, parent, guarantor, emergency contact, or other third party unless they are satisfied that the disclosure is authorized and limited to the information necessary for the purpose. Where there is uncertainty, the matter must be escalated to the Privacy Officer before information is released.

A record should be kept of the verification steps taken, the authority relied on, the information disclosed, the date of disclosure, and the person or organization to whom the information was disclosed.

13. Investigation Process

The Privacy Officer or delegate must conduct a fair and appropriate review based on the nature and seriousness of the complaint. The investigation may include:

- reviewing the complaint and relevant documents;
- identifying the applicable policy, procedure, system, record, or business process;
- interviewing or obtaining information from employees, managers, vendors, or service providers;
- reviewing system access logs, CCTV records, key fob/access records, portal records, emails, forms, or other records, where relevant and authorized;
- determining whether personal information was collected, used, disclosed, retained, corrected, accessed, or destroyed appropriately;
- assessing whether consent, notice, legal authority, or contractual authority existed;
- assessing whether safeguards were reasonable;
- determining whether a breach occurred;
- identifying any corrective action or process improvement required; and
- documenting findings.

The investigation must be limited to what is necessary to assess and resolve the complaint.

14. Confidentiality During the Complaint Process

Privacy complaints must be handled confidentially.

Information about the complaint may only be shared with individuals who on a need to know basis.

Employees involved in the complaint process must not discuss the complaint with others unless authorized by the Privacy Officer or delegate.

15. Access Requests

Where a complaint includes a request for access to personal information, the Privacy Officer or delegate must:

- confirm the scope of the request;
- verify the requester's identity and authority;
- conduct a reasonable search for responsive records;
- provide the information in a generally understandable format, where access is granted;
- explain abbreviations, codes, or system references where needed;
- explain in writing any refusal or partial refusal;
- advise the individual of available recourse; and

Access requests must generally be completed within 30 calendar days unless a lawful extension applies.

16. Correction Requests

Where a complaint includes a request to correct personal information, the Privacy Officer or delegate must:

- confirm the information the individual believes is inaccurate or incomplete;
- ask the individual to provide supporting information, where reasonable;
- determine whether the correction should be made;
- correct the information where appropriate;
- where appropriate, notify third parties to whom the incorrect information was disclosed;
- where the correction is not made, annotate the record with the correction requested but not made, where required or appropriate;
- explain the outcome to the individual in writing; and
- advise the individual of available recourse.

17. Complaints Involving Service Providers or Third Parties

Where the complaint involves a service provider, contractor, property owner, partner institution, technology vendor, payment processor, screening provider, or other third party, the Privacy Officer or delegate must:

- review the relevant contract, data processing terms, confidentiality obligations, or service arrangement;
- notify the third party only where appropriate and necessary;

- request information needed to assess the complaint;
- require the third party to preserve relevant records;
- assess whether the third party complied with contractual and privacy obligations;
- determine whether corrective action is required; and
- document communications and findings.

If the third party's handling of personal information may create legal, contractual, regulatory, or reputational risk, the Privacy Officer should consult legal counsel.

18. Complaints Involving Employees or Candidates

Where the complaint involves employee or candidate personal information, the Privacy Officer or delegate should involve HR only to the extent necessary to assess and resolve the matter.

Employee or candidate privacy complaints may involve:

- recruitment records;
- background or reference checks;
- payroll, benefits, or tax information;
- accommodation or medical information;
- performance or disciplinary records;
- electronic monitoring information;
- CCTV or access control records;
- employee file access; or
- disclosure of employee personal information to managers, vendors, or third parties.

Access to employee or candidate privacy complaint information must be restricted to those with a need to know.

19. Complaints Involving CCTV, Key Fob Records, or Security Logs

Complaints involving CCTV, key fob/access records, incident reports, or security logs must be handled carefully due to the potential involvement of multiple individuals' personal information.

The Privacy Officer or delegate must consider:

- the purpose for which the information was collected;
- whether the use or disclosure was connected to safety, security, access management, incident response, legal compliance, or another authorized purpose;
- whether access to the information was limited to individuals with a need to know;
- whether the records are still available under applicable retention practices;
- whether disclosure would reveal personal information about another individual;
- whether severing, redaction, or summary information is appropriate; and
- whether legal counsel should be consulted before releasing or refusing access.

20. Complaints Involving a Potential Privacy Breach

If the complaint suggests that personal information may have been lost, accessed without authorization, disclosed without authorization, or otherwise compromised, the Privacy Officer or delegate must immediately assess whether the matter is a potential privacy breach.

If a potential breach is identified, the Privacy Officer must:

- take immediate steps to contain the issue;
- preserve relevant records;
- follow UniLodge Canada's privacy breach response process;
- assess the risk of harm;
- determine whether notification to affected individuals, privacy regulators, law enforcement, insurers, contractual partners, or other parties is required;
- document the breach assessment and outcome; and
- continue to manage the complainant's concern through this Procedure, where appropriate.

21. Findings and Outcome

After reviewing the complaint, the Privacy Officer or delegate must determine whether the complaint is:

- substantiated;
- partially substantiated;
- unsubstantiated;
- inconclusive; or
- resolved informally.

The outcome should be based on the information available, applicable privacy law, the Privacy & Confidentiality Policy, related procedures, and reasonable privacy practices.

Corrective actions may include:

- correcting, deleting, annotating, restricting, or updating personal information;
- providing access to personal information;
- improving notices, forms, or consent language;
- limiting access permissions;
- retraining employees;
- updating procedures or workflows;
- addressing vendor or service provider issues;
- improving safeguards;
- changing retention practices;
- issuing reminders to employees or managers;
- escalating disciplinary concerns, where appropriate; or
- taking other reasonable steps to address the issue.

22. Response to the Complainant

The Privacy Officer or delegate must provide a written response unless the matter is resolved informally and the complainant agrees that no written response is needed.

The response should not disclose confidential business information, privileged information, personal information of another individual, or information that could compromise safety, security, an investigation, or legal rights.

23. Regulator Complaints or Investigations

If UniLodge Canada receives notice of a complaint, review, investigation, inquiry, or request from a privacy regulator, the Privacy Officer must be notified immediately.

The Privacy Officer will coordinate the response and may involve legal counsel, senior leadership, HR, IT, Operations, Finance, insurers, or external advisors as appropriate.

Employees must not respond directly to a privacy regulator unless authorized by the Privacy Officer or legal counsel.

24. Non-Retaliation

UniLodge Canada will not penalize, retaliate against, or treat an individual adversely because they raise a privacy concern or complaint in good faith.

Employees must not discourage an individual from making a privacy complaint or contacting a privacy regulator.

25. Complaint Records

The Privacy Officer or delegate must maintain a privacy complaint records. Complaint records must be stored securely with restricted access.

26. Retention of Complaint Records

Privacy complaint records should be retained for a reasonable period based on legal, operational, evidentiary, and risk considerations.

At a minimum, records should be retained long enough to demonstrate that UniLodge Canada received, reviewed, responded to, and resolved the complaint, and to allow the individual to exercise any applicable recourse rights.

Where a complaint involves a privacy breach, litigation risk, regulator complaint, employment matter, resident dispute, insurance issue, or contractual issue, records must be retained in accordance with applicable legal hold, breach record, or document retention requirements.

27. Reporting and Continuous Improvement

The Privacy Officer should periodically review privacy complaints to identify trends, recurring issues, training needs, process gaps, vendor concerns, or policy updates.

Where appropriate, the Privacy Officer may provide de-identified or summary reporting to senior leadership.

28. Availability of Complaint Process

Information about UniLodge Canada's privacy complaint process will be made available upon request where legislatively required. A Privacy Concern Process Summary document is available for external distribution.

29. Procedure Review

This Procedure should be reviewed at least every two years, or earlier if required for legislative or business purpose.

Appendix A – Privacy Complaint or Request Intake Checklist

The Privacy Officer or delegate should document:

- Date complaint received:
- Method received:
- Name of complainant:
- Contact information:
- Relationship to UniLodge Canada:
- Property, site, department, or system involved:
- Description of concern:
- Type of personal information involved:
- Date or date range of incident or concern:
- Is identity verification required?
- Is this an access request?
- Is this a correction request?
- Is there a potential privacy breach?
- Is a service provider or third party involved?
- Is legal counsel required?
- Acknowledgement sent:
- Assigned reviewer:
- Target response date:
- Outcome:
- Corrective actions:
- Date closed:

Appendix B – Complaint Acknowledgement Template

Subject: Privacy Complaint Received

Dear [Name],

Thank you for contacting UniLodge Canada. We have received your privacy complaint or concern dated [date].

Your matter has been referred to the Privacy Officer or an authorized delegate for review. We may contact you if additional information is needed to assess your concern.

We will handle your complaint confidentially and will involve only those individuals who need to know in order to review and respond to the matter.

We will make reasonable efforts to respond as soon as possible. Where your concern includes a request for access to or correction of your personal information, we will apply the applicable privacy law timelines.

If you have questions or wish to provide additional information, please contact:

Privacy Officer – UniLodge Canada
privacy@unilodge.ca

Sincerely,
[Name]
[Title]

Appendix C – Complaint Response Template

Subject: Response to Privacy Complaint

Dear [Name],

Thank you for raising your privacy concern with UniLodge Canada.

We have reviewed your complaint regarding [brief summary of concern]. As part of our review, we considered [brief high-level summary of steps taken, such as relevant records, systems, policies, or individuals consulted].

Based on our review, we have determined that [insert outcome: the complaint was substantiated / partially substantiated / not substantiated / inconclusive / resolved].

[Insert appropriate explanation of findings.]

Where appropriate, UniLodge Canada has taken or will take the following steps:

- [Corrective action, if applicable]
- [Process improvement, if applicable]
- [Training or safeguard improvement, if applicable]

For privacy, confidentiality, legal, or security reasons, we may not be able to provide all details of our internal review or information relating to other individuals.

If you are not satisfied with this response, you may contact the applicable privacy regulator, including *the [Office of the Privacy Commissioner of Canada]*, or specify the {applicable provincial body.}.

Sincerely,

[Name]

Privacy Officer or Authorized Delegate

UniLodge Canada

privacy@unilodge.ca

Document Control	Details
Document Type	Internal Procedure.
Related Policy, SOP, Guides and Tools	Privacy & Confidentiality Policy and Privacy Concern Process Summary CCTV and Video Surveillance SOP, Resident, Parent, Guarantor and Emergency Contact Disclosure Guide, System Access and Permissions SOP, Records Retention and Destruction Schedule.
Procedure Owner	Privacy Officer
Primary Users	Privacy Officer and authorized delegates; Human Resources, IT, Operations, site leaders, and legal counsel as required
Jurisdictions	Ontario, British Columbia, Alberta, and interprovincial/cross border activities where PIPEDA applies
Effective Date	June 2026
Version	1.0
Review Cycle	At least every two years, or earlier as required.