



Condo Control

PRIVACY & DATA PROTECTION

PIPEDA Compliance and Privacy Policy

Last reviewed · September 23, 2026



Contents

This document outlines how and why we collect personal information, how we protect it, and the procedures for making an inquiry or filing a complaint.

01	Overview	Our commitment and the purpose of this policy
02	Purpose of Data Collection	What we collect and how each element is used
03	Consent	How consent is provided and maintained
04	Use, Disclosure & Retention	Who can access your information, and for how long
05	Viewing & Updating Your Personal Information	Reviewing and correcting your records
06	Safeguards We Employ	Technical features, security procedures, contractual obligations
07	How to Contact Us	Contact details and our complaint process

01 Overview

This document outlines our commitment to protecting your privacy and personal information. We understand that privacy is important both to our clients and their owners, and we will take all necessary steps to safeguard the information that you entrust to us.

This document outlines our approach to privacy and information security. It explains how and why we collect personal information, how we protect the information, and the procedures for inquiring or filing a complaint.

This document is also provided to comply with the Canadian privacy legislation, the *Personal Information Protection and Electronic Documents Act*, commonly known as **PIPEDA**.

02 Purpose of Data Collection

In order to provide a full range of services to our clients, we require access to personal information about the owners and residents of the condominiums we service. The following table lists the data elements we collect and how each is used to provide our service.

TERMINOLOGY

In this section, the term "**Administrative Users**" refers to your board members or property managers.

#	DATA ELEMENT	HOW IT IS USED
1	Email address	Email addresses uniquely identify an individual user of our system and are used when clients log in. They are also used to send email notifications when a new document or piece of information is posted.
2	Condominium unit number	Most information in our system is organized by unit number — for example, it allows administrative users to easily identify which unit a service request relates to. It is also used to generate mailings when the unit does not have an off-site address.
3	Owner & tenant first and last name	Used by administrative users when they run reports from the system, and so that users can easily identify communication within the system — it is much easier for a property manager to respond to a service request when they know the name of the person who submitted it.
4	Off-site mailing address (if applicable)	If the unit is a rental unit and the owner lives off-site, an off-site mailing address is required to generate mailings and address reports.
5	Phone numbers	Required to make use of Condo Control's reporting features. If phone numbers are not provided, administrative users will not be able to look up phone numbers within the system.
6	Emergency contact information	These fields allow owners and residents to easily supply and update this information, so administrative users can quickly refer to it in the event of an emergency.

7	Vehicle information	Used by administrative users for reporting purposes. This includes make, model, and license plate information for resident vehicles.
---	----------------------------	--

WHY ALL UNITS ARE INCLUDED

The above information is required of all units — not just the units which use the system — in order to provide full functionality. Many features, like reports, will not provide full and useful information if the entire list of units and owners is not loaded into the system.

03 Consent

Upon commencing service with us, the board turns over current copies of the above personal information so that we may commence providing service. By turning over this information to us, the boards are providing their consent for us to use the information as outlined above.

In cases where owners provide updates to their own information through our online system, the online system explains how the information will be used.

04 Use, Disclosure & Retention

Your information will be used for the purposes outlined above; namely, it will be provided to your board members, property managers, or security guards so that they may carry out the administration of your condominium. (It is important to note that they will already have access to this information anyway; they are simply storing it in Condo Control.) In addition, we will use your information to provide email notifications when new information is available on your website.

NO MARKETING USE

Condo Control will **never** use this information to contact you for marketing or sales purposes, and will only contact you to provide support — for example, if you require assistance using our service and request that we email or call you.

We will also use your personal information to verify your identity, as required by PIPEDA, when you contact us with a request. For example, if you require us to reset your password, we will ask you to confirm several facts, such as your email address, name, and unit number.

Other than your board, property managers, and security guards, we will never disclose your information to a third party unless we have a suitable contractual agreement in place to protect your information. For more details, see **Sub-Contractor Agreements** under **Safeguards We Employ**.

In addition, personal information is not available to other owners in your condominium. Aside from administrative users (such as board members, property managers, and security guards), other owners can see only their own personal information.

RETENTION

We will retain your personal information in our active system only as long as you are an owner of a unit in a condominium which retains our services. If your condominium no longer uses our service, your information will be removed immediately from our active system.

05 Viewing & Updating Your Personal Information

Owners and residents may easily review the personal information we have about them and provide updates by signing into our online service and selecting the **"My Account"** tab.

Per PIPEDA, owners and residents may also request copies of their personal information in an alternative format. To initiate a request, please use the information in the **How to Contact Us** section of this document. When requesting a copy of your information, you will be required to provide enough information that we can verify your identity as outlined above.

06 Safeguards We Employ

We take several precautions to ensure that your data is safeguarded and will remain private. This section explains each step that we take.

Technical features

Encryption

All data transfers conducted in the normal course of business are encrypted to prevent unauthorized third parties from gaining access to your data. Your account password is stored using a "one-way hash" — only you (not even Condo Control employees) know your password.

Firewalls

All access to the "back end" functions of Condo Control is protected with a firewall to ensure that only authorized individuals have access.

Password length & lockout

Your Condo Control password must be at least 6 characters long. We will lock your account and require a password reset after 5 wrong attempts, to prevent unauthorized users from guessing your password.

IP address tracking

Whenever an end-user accesses Condo Control, we record their IP address so we can identify where the request came from. This assists us if a security-related investigation is required.

Two-factor authentication

For back-end services used by Condo Control as part of the offering, we enable and use two-factor authentication wherever possible.

Security procedures

- **Training.** All employees of Condo Control are required to complete training on PIPEDA to ensure they understand our obligations to protect your information.
- **Limited access.** Only employees who have a business need are given access to your personal information.
- **Physical access control.** Our servers are in a secure data centre facility in downtown Toronto. This location is disclosed only to Condo Control employees. All premises have sufficient physical security measures in place to ensure the confidentiality of your data.
- **SAS 70 certification.** We use Amazon Web Services (AWS) as a backup hosting provider if our primary servers ever experience a failure. AWS is SAS 70 certified on an annual basis; this certification is reviewed annually by a third party and ensures that appropriate controls are in place to limit the risk to your information. For full details, visit aws.amazon.com and click the "Security" link.

Contractual obligations

- **Client agreements.** Our standard client agreement, which all clients sign before commencing service, contains a section that outlines our confidentiality obligations to protect their information.
- **Employment agreements.** Our employees agree to be bound by this policy and adhere to everything contained within it. Failure to comply with this policy is grounds for discipline up to and including termination of employment.
- **Sub-contractor agreements.** From time to time, we may work with third parties to conduct our business. Third parties will only be given access to personal information if absolutely required, and in these cases they will be contractually obligated to follow this policy. In addition, we will conduct due diligence to ensure the contractor has sufficient safeguards in place to protect your information.

07 How to Contact Us

If you would like to contact us about anything contained within this policy, please use the information below:

EMAIL	contact@condocontrolcentral.com
PHONE	1-888-762-6636 · Select option 2 from the main menu
POST	Condo Control — Attention: Privacy Officer 2 Carlton Street, Suite 1000 Toronto, ON M5B 1J3, Canada

Complaint process

We take all complaints very seriously, including complaints about information security or privacy. If you have a complaint, we will follow this process to address it:

- 1 We will acknowledge your complaint within **2 business days**.
- 2 We will ask you for more information and clarification as needed to complete an investigation.
- 3 We will conduct a thorough investigation and advise you of the results.
- 4 We will communicate the results of our investigation to you.
- 5 We will take corrective action and revise our policies and procedures as required to address the problem.

As required under PIPEDA, in most cases we will conduct this investigation and advise you of the results within **30 days**. If more time is required, we will advise you of this within 30 days and complete the investigation within **60 days** from your original complaint.

ESCALATION

In the unlikely event that your complaint is not resolved to your satisfaction, you may contact the Privacy Commissioner of Canada. The Office of the Privacy Commissioner may be reached on the web at priv.gc.ca.