PIPEDA COMPLIANCE AND PRIVACY POLICY

Last Reviewed: April 15, 2021

OFFICE CONTROL
WORKPLACE MANAGEMENT MADE SIMPLE

Contents

This document outlines our commitment, policies and procedures for safeguarding your personal information and ensuring our compliance with Canadian privacy law.

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 outlines 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, *Personal Information Protection and Electronic Documents Act*, commonly known as PIPEDA.

This policy is reviewed annually and updated as needed. The next review is scheduled to be completed before April 1, 2022.

Purpose of Data Collection

In order to provide a full range of services to our clients, we require access to personal information about the tenants of the buildings which we service. The following table lists the data elements that we collect and how we use the data to provide our service.

In this section, the term "Administrative Users" refers to office, property, or facilities managers.

	Data Element	How It Is Used
1	Email Address	Email addresses are used to uniquely identify an individual user of our system and are used when clients log into our system. In addition, email addresses are used to send email notifications when a new document or piece of information is posted.
2	Office Number	Most information in our system is organized by office address numbers. For example, having this information allows administrative users to easily identify which office a service request is related to. This information is also used to generate mailings if the office does not have an offsite address.
3	Tenant First and Last Name	This information is used by administrative users when they run reports from the system. It is also used so that users can easily identify communication within the system. For example, like #2, it is much easier for a property manager to respond to a service request if they know the name of the person who submitted it (rather than just the email address or office number).
4	Off-site Mailing Address (If applicable)	If there is an off-site mailing address for an office, the address will be used to generate mailings and address reports.
5	Phone Numbers	Phone numbers are required to make use of Office Control's reporting features. If phone numbers are not provided, then administrative users will not be able to lookup phone numbers within the system.
6	Emergency Contact Information	Emergency contact information fields are used so tenants can easily supply and update this information. Administrative users can quickly and easily refer to it in the event of an emergency.
7	Vehicle Information	Vehicle information is used by administrative users for reporting purposes. This information includes make, model, and license plate information for vehicles.

The above information is required of all offices, not just the offices that 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 offices and tenants is not loaded into the system.

Consent

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

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

Use, Disclosure & Retention

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

Office 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 you 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, office number, and so-on.

Other than your office, property and/or facilities managers, 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" below.

In addition, personal information is not available to other tenants in your building. Aside from administrative users, other tenants can only see their own information.

We will retain your personal information in our active system only as long as you are a tenant in a building or workplace that retains our services. If your building no longer uses our service, your information will be removed immediately from our active system.

Viewing and Updating Your Personal Information

Tenants 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 the PIPEDA, tenants may also request copies of their personal information via 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.

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. In addition, your account password is stored using a technique called a "one way hash". This means that only you (not even Office Control employees) know your password.
- **Firewalls.** All access to the "back end" functions of Office Control is protected with a firewall to ensure that only authorized individuals have access.
- **Minimum password length and password lockout.** Your Office Control password must be at least 6 characters long. In addition, we will lock out your account and require you to reset your password if 5 wrong passwords as submitted. This is to prevent unauthorized users from guessing your password.
- **Tracking of IP Addresses.** Whenever an end-user accesses Office Control, we record their IP address so that we can identify where the request came from. This assists us in the event that a security-related investigation is required.
- **Two-Factor Authentication.** For back-end services used by Office Control, we enable and use two-factor authentication wherever possible.

Security Procedures

- **Training.** All employees of Office Control are required to complete training on the 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 Office 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, and 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 http://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.

How to Contact Us

Contact Details

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

Via email: contact@condocontrolcentral.com

Via Phone: 1-888-762-6636. Select option 2 from the main menu.

Via Post: Office Control
Attention: Privacy Officer
2 Carlton Street, Suite
1000
Toronto, ON M5B 1J3
CANADA

Complaint Process

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

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

As required under the 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.

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 http://www.priv.gc.ca/.