Tenant Data Privacy Policy: Keyless Entry System

Effective Date: February 1, 2022

As a part of the configuration of the keyless entry (smart access) system at Greene Avenue Condominium, certain user information minimally necessary for the operation of the system is stored and logged on an ongoing basis.

What kind of data is stored?

The ID number of each key fob is stored within the system, and is associated only with its unit's building and apartment number.

The names of unit owners or residents have NOT been entered into the system, and are neither known to, nor stored by the system.

For example, the key fobs for unit 317/3B are only associated with that unit's building/apartment number, and NOT with any specific person living in that unit nor any person who may make use of the key fob.

What kind of data is logged?

When a key fob is used to open the front door by swiping on the reader, the unique ID number of that key fob, along with the time and date it was used are logged by the system.

For example, the system may log that a key fob from 317/3B was successfully used at 4:25pm on October 25th., but will have no way of knowing nor logging the identity of the person who actually used the key fob.

When the front door is "buzzed" open via the intercom inside of a unit, only a generic "door open" request for that building's front door is logged by the system. Data about which specific unit buzzed open the door is neither known nor logged. When any person leaves the building through the front door by manually opening the door, no information of any kind is logged by the system.

How long is data stored?

Key fob registration info (ID numbers and the respective units) is stored ongoingly, but will be destroyed or anonymized within 90 days after the unit owner or resident permanently vacates the apartment building.

Entry/exit data logged by the smart access system will be destroyed or anonymized within 90 days after collection or generation.

Data necessary to debug or repair the system, or necessary to detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, may be held longer.

Who can access the smart access system data?

Access to the data from the smart access system is strictly limited to the managing agent of the property, and to the building's board of managers. The data shall not be sold, leased, or otherwise disclosed to another person except as required by law or order of a court.

Security of the data.

Electronic access to the data is protected through the use of industry strength passwords. The software and firmware of the components shall be maintained and updated regularly.

Even though no specific personal information is stored in the smart access system, in the event of a data breach, notification will be made as soon as determined safe to do so.