VERGE SENSE

# Workplace Assistant

Security & Privacy Whitepaper

MAY 2024

# Contents

# Introduction

At VergeSense, we take privacy seriously. Our commitment to safeguarding our customers' data is always top of mind, including  as we engineer and launch our new Workplace Assistant application. This application is designed to enhance the way our customers interact with their occupancy data.

This whitepaper outlines the privacy measures and security protections in put in place for users of Workplace Assistant.

# Data Handling & Privacy

## Data Access Control

**User Opt-In**
Workplace Assistant operates on a strictly opt-in basis. Users must manually export their data from the VergeSense platform and upload it into the AI Assistant.

This allows users to choose specifically what data gets shared with the AI Assistant and ensures complete separation from our analytics platform and data collection systems.

**Session Based Access**
Each Workplace Assistant chat session is scoped only to the data the end user has uploaded for that session. The AI Assistant does not have access to data used across other historical sessions, it has no way to query databases outside of the user uploaded dataset for the specific session.

**Completely Isolated**
The Workplace Assistant is architected such that it has no access to any data in the VergeSense platform. Each session only has access to the data the user opts-in to use for analysis and provides answers based on the vast amounts of knowledge and context upon which it was trained.

## Data Anonymity

**Anonymized Data**
Data exported from the VergeSense platform DOES NOT contain customer names or any personally identifiable information, aside from space and building names which are necessary for meaningful data analysis.

These unique identifiers do not explicitly disclose to whom the data belongs, ensuring customer data remains anonymous.

# Data Handling & Privacy

## OpenAI Enterprise Privacy Policy

**Ownership and Control:** By utilizing the OpenAI API, we benefit from the OpenAI Enterprise Privacy Policy, ensuring users maintain ownership and control over their data. This includes a commitment not to train on user business data, offering enterprise-level authentication, and providing fine-grained access control.

**Security and Compliance**
Both VergeSense and OpenAI meet SOC2 compliance standards and employ robust data encryption methods both at rest and in transit. VergeSense also has ISO27001 certification, performs annual pen test and is trusted by numerous global enterprises.

**Trusted by Enterprise**
We use the same model and API technology from OpenAI that powers Microsoft Copilot and various other enterprise AI applications.

# Generic Training Data

**Anonymity in Training**
All training data examples used within our system are generic and anonymized, consisting of example questions paired with example database queries only. There is never any possibility of customer data being used for training.

# Architectural Overview

Providing an overview of the system architecture offers visibility into the privacy and security measures inherent in the design of our AI system.

**Data Export and Upload**
Users export their occupancy data from the VergeSense Occupancy Intelligence platform, resulting in data already void of personally identifiable information, except necessary space and building names.

**Data Interaction**
This data is then uploaded by the user into Workplace Assistant, where it is securely attached to threads for analysis.

The system combines this data with context (e.g., column descriptions, generic example queries, and corporate real estate knowledge) to facilitate meaningful interactions and responses.

**Analysis and Visualization**
Leveraging the OpenAI Assistants API, the system analyzes the uploaded data, enabling users to query, visualize, and gain insights into their occupancy trends and patterns.