Occuspace Inc.

Last updated on 5/26/23

Privacy and Permissions Management Document

Introduction

This Privacy and Permissions Management document outlines the principles and practices employed by Occuspace to safeguard user information and permissions within our software application and sensor network. Occuspace takes consumer privacy very seriously, and that principle has been incorporated into the technical architecture of the product at a very fundamental level. Our objective is to ensure compliance with all relevant privacy laws and regulations, foster user trust, and provide transparency in our operations.

Data Collection and Usage

2.1. Types of Data Collected

Occuspace has two distinct types of users on which data is collected and who are covered by our privacy policy and procedures. Each user type is outlined below along with the data points that are collected.

Platform Customers
These individuals are contracted customers of the Occuspace service and are provided access to the Occuspace analytics platform and data. For these individuals the following information is collected to facilitate login and communications:

- Name
- Email
- Job Title (optional)

Occupants (Sensor Data)
This is the observed population in spaces monitored by Occuspace sensors, and that are accounted for in the reported occupancy data. Occuspace never connects to any devices of any individuals, and does not track or have the capability to track individual activity. All data collected in this category is non-personal or anonymous data and consists of:

- Randomized/Hashed ID from Bluetooth and WiFi devices
- Received Signal Strength Indicator

2.2. Purpose of Data Collection

Platform Customers

- The sole purpose of data collected in this category is for account creation and login on the Occuspace web dashboard, allowing users to access data for spaces they have permission to view

Sensor Data

- Occuspace collects this data to generate anonymous analytics on the presence of people in an area. No personally identifiable information (PII) is ever collected. Occuspace reports data for spaces 2,500 square feet and larger, ensuring individual desks or offices remain unreported.

2.3. Legal Basis for Data Processing

Platform Customers

- Consent: All users on the Occuspace platform provide their information voluntarily during the account sign-up process.
- Contract fulfillment: Occuspace requires this information to generate accessible and properly secured/authenticated accounts for customers

Sensor Data

- Legitimate interests: Occuspace utilizes data to help customers enhance visitor experiences, reduce real-estate costs, optimize workplace planning, and lower energy consumption. No personally identifiable information (PII) is ever captured.
- Contract fulfillment: Occuspace collects this information to generate utilization data for customers.

2.4. Data Retention

Platform Customers

- Occuspace retains user information for as long as users maintain an Occuspace account.

Sensor Data

- Aggregated utilization data: Occuspace stores anonymous, aggregated utilization data indefinitely to improve machine learning algorithms over time.

<u>User Permissions</u>

3.1. Consent

Platform Customers

- Platform Users have the right to delete their Occuspace account at any time, resulting in immediate deletion of all personally identifiable data.

Sensor Data

- All occupants have the right to disable Bluetooth and WiFi on their devices to prevent data capture by Occuspace sensors. Personally identifiable information (PII) is never collected.

3.2. User Control and Preferences

Platform Customers

- All Platform users can update their personal information and controls at any time via the Occuspace Web Portal available 24x7x365
- User accounts can be fully deleted and removed from the Occuspace platform via this Web Portal

Sensor Data

- Personally identifiable information (PII) is never collected by the Occuspace platform.
- All occupants have the right to disable Bluetooth and WiFi on their devices to prevent data capture by Occuspace sensors.

4. Data Security

- Occuspace's platform uses industry best practices around automation, immutability, isolated networking, fine grained access control, multi factor authentication, and least privilege permissioning
- All occupancy sensor data collected by Occuspace is encrypted during transit, and stored in an encrypted format when at rest. Access to the data is further restricted according to "least privilege" permissioning philosophy (see below).
- Occuspace maintains an internal set of policies, user groups, and associated mappings to functions that enforce the security practices at Occuspace. Our approach leverages the principles of "least privilege" advocated as a best practice by the software development industry today. Users (both actual and programmatic) are assigned only the minimum level of permissioning necessary to accomplish their designated tasks and no more, and only for the time that such permissioning is needed. When a user no longer needs specific access to a function the associated permissioning is revoked. Extremely fine grained access control is leveraged to ensure the proper granularity of permissions. All user permissioning is regularly reviewed via both administrative teams as well as automated controls.
- MFA is enforced for all employees of Occuspace, for both GUI and CLI control interfaces. There are zero exceptions to this rule. Occuspace religiously follows the usage of MFA for all systems and employees, even non-technical and non-privileged
- The Occuspace Technology Platform is highly segmented to isolate systems and traffic, and limit the "blast radius" of performance and security issues. The network topology makes heavy use of public and private subnets, ensuring that only components that need to have external access are in such an arrangement, while components that do not

need external access are never allowed to do so. Different platform components are isolated within their own network subnets, with interoperability provided only where it is required for normal operation. Traffic from component to component is explicitly permissioned down to the specific IP address and port level, following the "least privilege" permissioning principle.

5. Third-Party Sharing

Platform Customers

- No personally identifiable information is ever shared with third parties. This information is only maintained by Occuspace to provide secure and accessible access to Web analytics data.

Sensor Data

- Aggregated, normalized, and anonymized occupancy data may be shared with third-parties for the purpose of research, trend and comparative analysis. Data shared at this level is always aggregated from all Occuspace customers and is fully anonymized.

6. User Rights

Platform Customers

- Platform Users have the right to delete their Occuspace account at any time, resulting in immediate deletion of all personally identifiable data.

Sensor Data

- All occupants have the right to disable Bluetooth and WiFi on their devices to prevent data capture by Occuspace sensors.

7. Updates to the Privacy and Permissions Management Document

- All Platform Customers will be notified via email of any changes made to the Privacy and Permissions Management Document.
- A current up-to-date version of the Privacy Policy is always publicly available on the Occuspace Website.

8. Contact Information

- For any questions regarding this policy, please reach out to info@occuspace.io.

9. Compliance with Applicable Laws and Regulations

- Occuspace is committed to adhering to all relevant privacy laws, regulations, and industry standards to maintain and protect the privacy of all users and occupants of spaces monitored by Occuspace sensors.