innerspace

Privacy & Security Fact Sheet

Anonymity is not just a feature but a foundation of InnerSpace, protecting user identities at every level

Here at InnerSpace, we understand that workplace teams want to use space utilization insights to design better environments—not to compromise privacy.

That's why our platform is built from the ground up to provide actionable data while ensuring the anonymity and security of everyone in the space.

Information Security Management ISO 27001 Certified

GDPR COMPLIANT

GDPR LOCAL Certified

InnerSpace has been engineered to be anonymous-by-design and secure-by-design

We combine patented technology and advanced AI to deliver the real-time accuracy organizations need without collecting or exposing personally identifiable information (PII).

This document outlines the privacy-centric features and robust security architecture of InnerSpace. It is designed to be accessible to both technical and non-technical readers.

Private by Design
We collect only necessary occupancy data, with no PII stored.

MAC addresses are anonymized, ensuring no cross-location tracking.

Data Aggregation
Data is presented in aggregate form and fully anonymized to protect identities and comply with GDPR standards.

Robust Security
Our systems undergo regular audits and are certified to ISO27001 standards.

Secure Storage
Customer data is stored securely in Microsoft Azure with encryption and strict access controls.

If you have any questions about the content in this document, please don't hesitate to contact us at privacy@innerspace.io. Our team is here to help.

Completely Anonymous Data Collection

We leverage existing Wi-Fi infrastructure, avoiding cameras or raw sensor data, to collect only essential occupancy and space usage data.

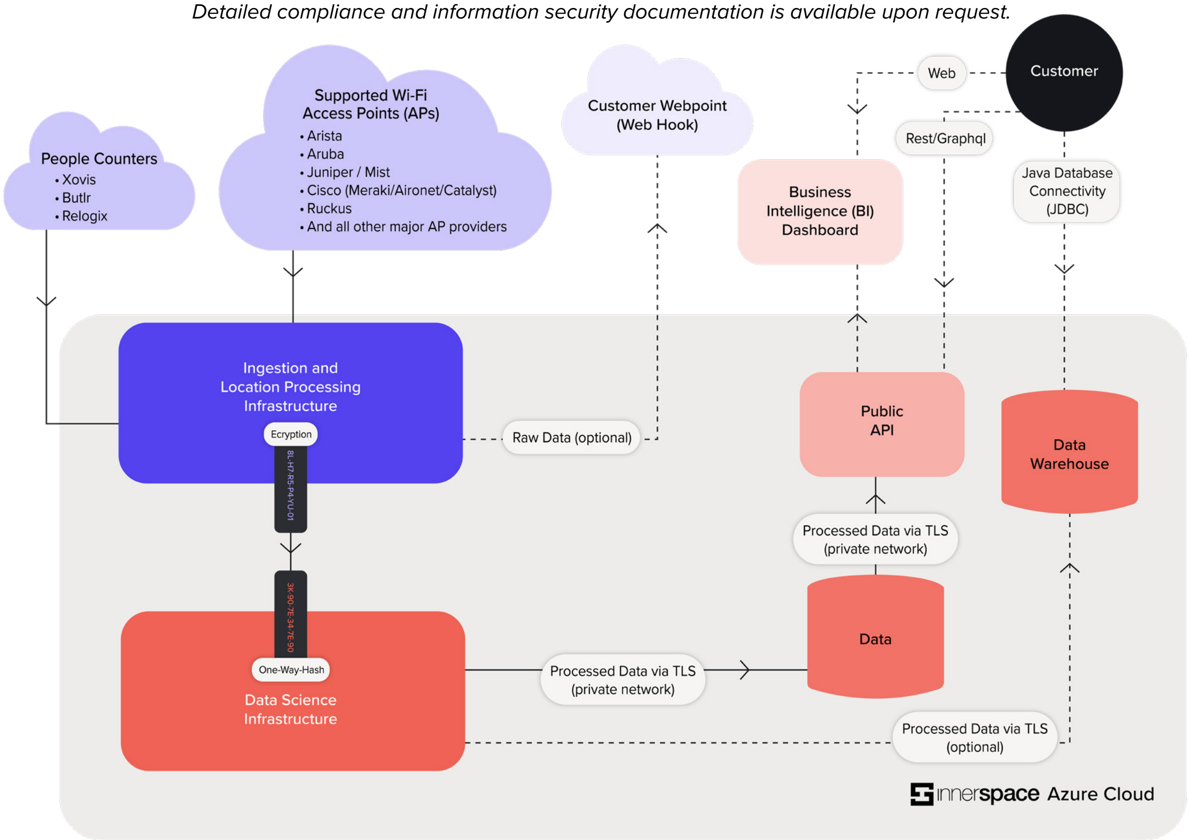
- Using one-way hashing, MAC addresses are anonymized with client-specific salts to prevent reconstruction or cross-location tracking.
- Aggregated behavioral patterns ensure individual identities remain protected.
- Compliant with GDPR and industry best practices, InnerSpace delivers secure, privacy-first workplace insights.

How our Anonymous Data Processing works

All data processing systems operate within a virtual private cloud, isolated from external access to ensure maximum security. This secure environment ensures data is highly protected and processed anonymously. InnerSpace is also certified to the ISO27001 information security standard.

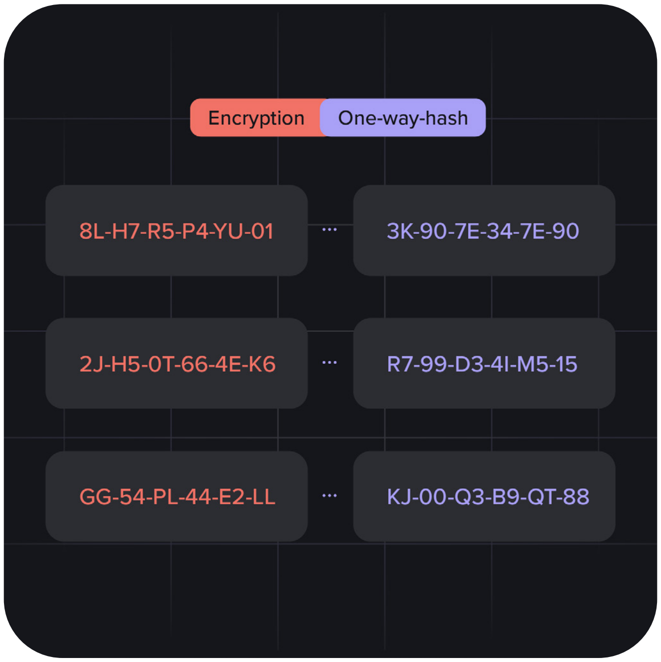
This involves an independent audit confirming that our security practices, policies, procedures, and operations meet or exceed industry standards for protecting customer information. To maintain these standards, we conduct regular security assessments and leverage industry-standard tools and processes.

Detailed compliance and information security documentation is available upon request.


People Counters
• Xovis
• Butlr
• Relogix
Supported Wi-Fi Access Points (APs)
• Arista
• Aruba
• Juniper / Mist
• Cisco (Meraki/Aironet/Catalyst)
• Ruckus
• And all other major AP providers
Customer Webpoint (Web Hook)
Web
Customer
Rest/Graphql
Business Intelligence (BI) Dashboard
Java Database Connectivity (JDBC)
Ingestion and Location Processing Infrastructure
Ecryption
8L-H7-R5-P4-YU-01
Raw Data (optional)
Public API
Data Warehouse
Processed Data via TLS (private network)
3K-90-7E-34-7E-90
One-Way-Hash
Data Science Infrastructure
Processed Data via TLS (private network)
Data
Processed Data via TLS (optional)
innerspace Azure Cloud

How our Data Encryption works

Existing Wi-Fi infrastructure (on-prem or cloud) connects to the InnerSpace cloud (Microsoft Azure's East US region) via the location service connector, which directly integrates with our spatial intelligence pipeline. This pipeline uses machine learning to derive sophisticated insights from the raw location data. This is via Transport Layer Security (TLS).



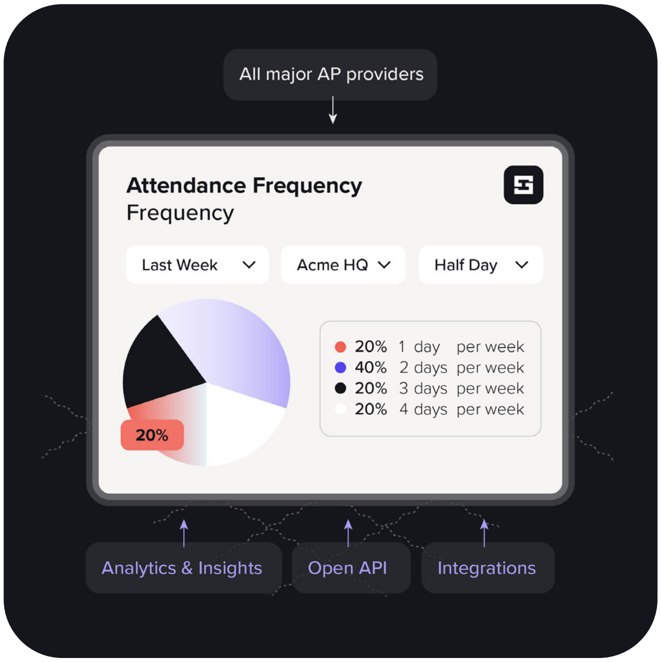
Anonymizing Personal Identifiable Information (PII)
The only personally identifiable data our systems process is a device's MAC address. No names, user IDs, or other personal identifiers are ever captured, processed, or stored. MAC addresses are anonymized instantly using a one-way hash with client-specific salts, and the original MAC address is discarded immediately. One-way hashing makes it virtually impossible to reverse-engineer the original MAC address. Client-specific salts ensure the same MAC address generates a unique hash at different client locations, preventing cross-location tracking.

Anonymity-First Data Processing
InnerSpace takes extra precautions to prevent identity inference—the ability to deduce someone's identity based on behavior. All data is presented in aggregate form, with individual behavioral patterns, such as movement pathways or locations, carefully anonymized to ensure identities remain protected.

Artificial Intelligence/Machine Learning (AI/ML)
InnerSpace ingests anonymous Wi-Fi location data and processes it using AI-powered algorithms on our cloud platform. Our proprietary engine ensures precise positional stitching between access point detections, delivering seamless full-floor coverage without duplication.

Real time updates to analytics & Building Management Systems/Integrated Workplace Management Systems (BMS/IWMS) integrations
After processing and normalizing real-time Wi-Fi location data against the mapped floor plan, the data is pushed to both our real-time API feed and BMS/IWMS integrations, including calendars, booking systems, communication apps, and more.

This processing happens in near real-time, with people count data updated every minute for actionable decision-making.



What Data Do we Capture?

We capture the following types of data:

- **Building and Floor Information:** This includes building and floor names, floor plans, access point (AP) layouts, and zone configurations.

- **Wi-Fi Telemetry Data:** This consists of anonymized MAC addresses, RSSI (Received Signal Strength Indicator), signal strength, timestamps, Wi-Fi bands, and access point details.

We Ensure the Highest Standards for Data Security

InnerSpace technology has been designed and developed to ensure your privacy is protected and data security is never compromised.
Every component of the InnerSpace platform including on-site networking technology, cloud-hosted infrastructure, software, and APIs, has been carefully engineered to securely capture, process, transmit, and store data.

- All data processing occurs within a virtual private cloud, inaccessible to the outside world, ensuring secure data handling
- Regular security assessments and industry-standard tools are used to protect customer data
- Data is stored in the Microsoft Azure cloud (East US region) with multiple layers of security, including encryption in transit and at rest
- InnerSpace is GDPR compliant ISO27001 certified, with independent audits verifying security practices and policies
- Only device MAC addresses are processed; no names, user IDs, or other identifiers are ever captured, processed, or stored
- MAC addresses are immediately anonymized using one-way hashing with client-specific salts, and the original MAC address is discarded
- One-way hashing ensures the original MAC address cannot be reconstructed, and client-specific salts prevent cross-location tracking
- Data is provided only in aggregate form, and behavioral patterns (e.g., pathways or locations) are obfuscated to protect individual identities
- Additional measures are in place to prevent identity inference, ensuring complete anonymity

Have a question about privacy or data security? Reach out to our team at privacy@innerspace.io