



FACT SHEET

Privacy & Security

How Locatee provides valuable workspace insights in compliance with data protection regulations.

As new technologies continue to emerge and reshape the world we live in, topics surrounding data privacy and protection are becoming ever more important. At Locatee, our mission is to empower corporate real estate leaders and decision-makers to make the best possible workplace decisions through the smart use of data. With that said, we are fully committed to the privacy and security of individual employees and enact strong measures to comply with local and international privacy regulations such as the European Union's General Data Protection Regulation (GDPR), which applies to all EU-based businesses as well as anyone processing the personal data of EU citizens.

How Locatee measures office occupancy

Locatee collects information in one of two ways: via the company's Wi-Fi and LAN network or, alternatively, through the use of sensors. Wi-Fi and LAN can be used to detect connections made to the network from an employee device such as a laptop, tablet, or mobile phone. In the case of sensors, it is not the devices which are being detected, but movement. In both cases, Locatee Analytics does not display continuous

Locatee tracks usage, not people



Locatee analytics measures the way office spaces are being used by the entire organisation. It does not track individual employee behaviour in the workplace.

information about any single device or any person, and all personal data are deleted after 24 hours. In this way, the solution provides workspace insight at no expense to employee privacy.

The right to opt out

A useful feature Locatee provides through its Smart Space mobile app is Colleague Finder. Colleague Finder indicates the general whereabouts of a coworker based on recent device connectivity. It is a feature that many teams find indispensable when working in large, complex teams. Nevertheless, employees always have the option to opt out of being found through the Colleague Finder. Furthermore, no historical data about an individual colleague's location can ever be viewed on Colleague Finder.

Locatee's commitment to protecting employee privacy



Locatee is GDPR-compliant and enacts strong measures to ensure the proper **encryption and anonymisation of personally identifiable data**.



Locatee removes any identifiers which can be traced to an individual employee. For any teams with fewer than 10 employees, Locatee displays a higher level of abstraction.



Data remains in control of the company. The collection, processing, and visualisation of data by Locatee is a service and has no effect on the ultimate ownership of the data.



Insights are provided via a web interface which is **protected by role-based access control**. Only authorised personnel may analyse the data collected and processed by Locatee.

Anonymisation and encryption of data

Locatee maintains a strict stance with regards to data protection and enacts strong measures to ensure that data is properly encrypted and anonymised. Data in transit is always protected using a TLS-encrypted HTTPS protocol, and data at rest is always encrypted. In addition, all the data collected are anonymised using a cryptographic one-way hash which adheres to the stipulations laid out in the EU GDPR. Therefore, even in a case of unauthorised access at the database level, it is not possible to retrieve the personal information of employees. Locatee removes any identifiers which can be traced to an individual, saving only irreversibly anonymised and aggregated data.

Aggregation and abstraction of data

When data is displayed on a team level, Locatee makes sure that each team consists of at least 10 members. For any teams of fewer than 10, data will only be available at a higher level of abstraction. This is to prevent the possibility of making statements about the behaviour of any individual employee through the principle of exclusion. In the case of the Colleague Finder feature in Locatee's Smart Space app, employees reserve the right to opt out of being found, and individual data is not stored for historical analyses.

Ownership of data

The information gathered on customer premises is transferred over a TLS-encrypted HTTPS REST interface to Locatee's ISO 27001-certified data centres on Google Cloud Platform, where they are then securely processed and anonymised using state-of-the-art technology. The service of collecting, processing, and visualising data by Locatee has no effect on the ownership of the data, which remains in control of the company. Locatee does not own, distribute, or sell any of the information it gathers.

Access to data

Workplace insights are provided via Locatee Analytics, which is a protected web interface. To prevent the potential misuse of data, Locatee uses a role-based access model to ensure that only authorised personnel may analyse the data collected and processed.

Transparent communication

We firmly believe that more transparency fosters more understanding, so apart from technical and organisational measures, we take care to involve every stakeholder about Locatee's services, policies, and terms and conditions.

How anonymisation works in Locatee

1

Data is collected from LAN, Wi-Fi, and sensors

- Data from devices connected to LAN or Wi-Fi is collected
- For each connected device the unique MAC address and the timestamp of the measurement is transmitted.
- If sensors are used, Locatee receives occupancy data from sensors
- All data is sent to Locatee's ISO 27001-compliant data centres

LAN/Wi-Fi detects devices



Sensors detect occupants



2

Individual user information is anonymised

- MAC address and personally identifiable information like usernames are anonymised using a salted SHA-512 hash function
- Sensor data do not contain user information and don't require anonymisation
- The same user data is hashed with a new salt each day; using this method, it is impossible to connect an employee's current location with historical data.

Data is anonymised



3

Anonymised data is stored

- No personally identifiable information is stored for more than 24 hours
- Whenever historic data is accessed, only information on workplace utilisation can be retrieved; no user profiles can be built or deduced

Hashed data is stored



35d91262b3c3ec88
41b54169588c97f7

«Safeguarding our employees' privacy is top priority for us. Thankfully, it is for Locatee as well. We have access to valuable insights, but Locatee Analytics still ensures maximum data protection.»

Carine Bommeli

Innovation and Projects, Swiss Post Real Estate

Locatee is the leading workplace analytics solution that empowers you to make decisions about your real estate portfolio with confidence.

We look forward to hearing from you.

Locatee AG
Albisriederstrasse 243a, 8047 Zurich, Switzerland

+41 43 508 51 23
info@locatee.com, www.locatee.com