# Data protection

This document describes how different types of data are handled by MazeMap. These different types of data are described as well.

Overview

Figure 1 illustrates MazeMap's architecture. MazeMap is a cloud based service that users can interact with in two different ways. End users can use the 6: Wayfinding application to interact with the indoor maps, and super users can edit the maps using the 7: Map Editor. Both the 6: Wayfinding application and the 7: Map Editor interact with 5: Indoor map service.
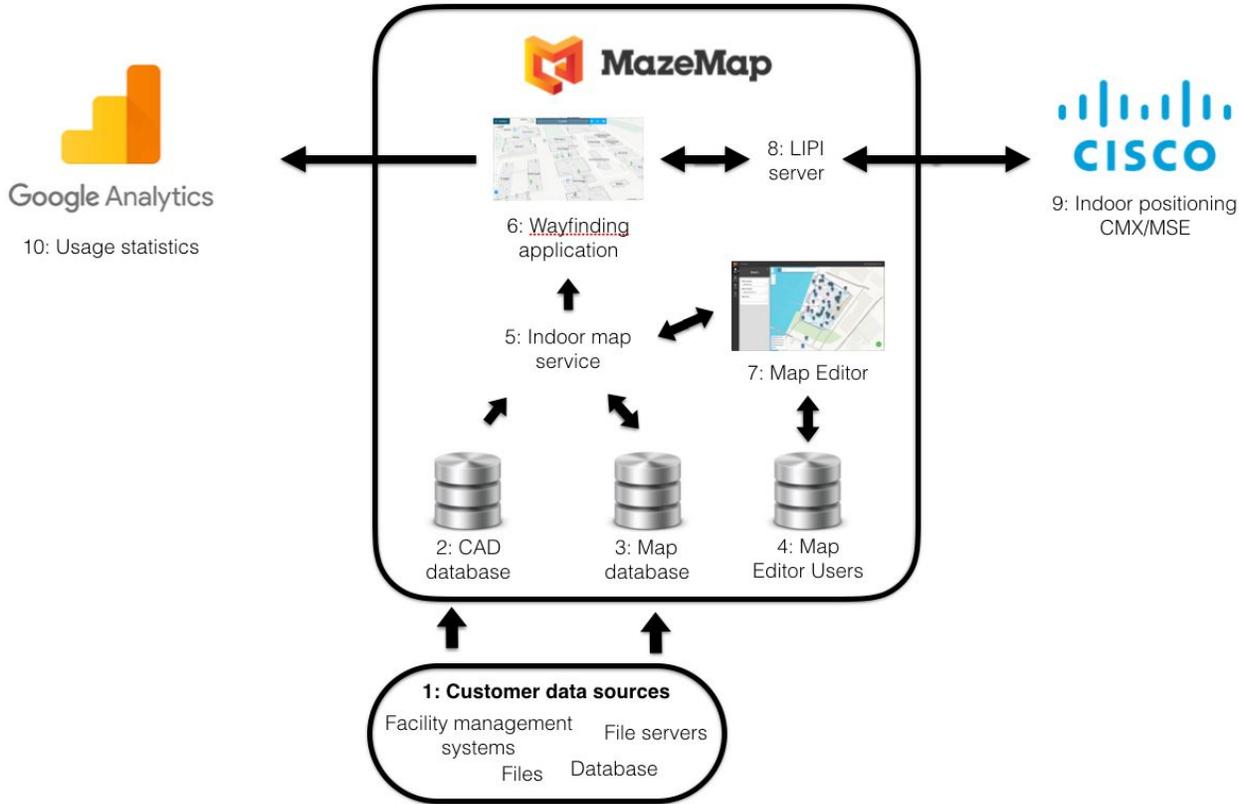
Figure 1: MazeMap architecture.

The 5: Indoor map service reads data from 2: CAD database and 3: map database. 2: CAD database stores the CAD files that are provided to MazeMap by customers, and 3: map database contains the finished map including meta data such as points of interest information. Both the CAD files that are the source for the map making process and the meta information that is used to populate the map with points of interest information are provided by the customer through 1: Customer data sources. The source data can be provided in many different ways, such as through facility management systems, file servers, databases and more.

The 7: Map Editor allows super users to edit POIs and paths. MazeMap stores information about the super users (user name and hashes of passwords) in the database 4: Map Editor Users for authentication purposes. This is the only part of MazeMap that maintains any user information.

The 6: Wayfinding application interacts with two services that stores user data: 9: Cisco CMX/MSE and 10 Google Analytics.

In the next sections, the different components and the data they store will be presented.

1: Customer data sources

Customer data can be read from facility management systems, files, file servers and databases that are maintained by the customer itself. MazeMap follows the protocol used by the customer.

2: CAD database

CAD files stores the technical building plans, typically with technical room numbers and sometimes room names. The files can contain sensitive information, such as lab names, the electrical systems and more.

Because of the sensitive nature of the information stored in CAD files, the CAD files that are received from customers are stored in a data center in Norway hosted by [zetta.io](). The data protection provided by zetta.io includes SSL encryption in flight and AES encryption at rest. The physical location of the data centres have high grade fencing with secure access control and both internal and external security surveillance camera systems. All of the facilities are fully compliant with the International Organisation for Standardisation (ISO) recognised standards for quality, security, safety and environmental management. These includes ISO 9001, ISO 27001, ISO 14001 and OHSAS 18001.

Norway is chosen as the location for the data center as Norwegian Privacy Laws are some of the most restrictive in the world. Information will not be shared unless there exist a Court Order.

Only a subset of the developers and delivery personnel with administrative rights at MazeMap have access to this data. Currently, this is restricted to a total of ten people.

3: Map database

The map database stores the information that is used to draw a map. This includes the information that are generated automatically by MazeMap by interpreting the CAD files as well as the POI information that is provided by the customers. Both paths and POIs can be autogenerated by the MazeMap and manually edited by super users.

The Map database runs on Microsoft Azure, which is Microsoft's cloud offering. The map database stores only the data that will be shared in the map, so the data is less sensitive than the CAD files, as the CAD files typically contain more data than what is going to be shared in the maps.

Developers and a subset of the delivery personnel in MazeMap have access to this data. The data is also accessible to the personnel given the access rights for managing POI information in the MazeMap Map Editor by the customer.

4: Map Editor Users

User names and hashes of passwords are stored in a database in the Azure cloud. The passwords themselves are not stored in the cloud.

5: Indoor map service

The indoor maps that are generated by MazeMap are shared through the MazeMap mapping and wayfinding service to end users. Two types of indoor maps are supported, which are public maps and private maps.

Public maps are shared with anyone and can be integrated in any web pages. By default the maps are shared on use.mazemap.com and in MazeMap's mobile apps for Android and iOS.

Private maps are only shared to applications and services that provide MazeMap's API with a private authentication key. Typically, the maps can be shared in third party mobile apps (not the MazeMap mobile apps) and internal web pages hosted behind a firewall by a customer. Further documentation on how private maps work can be requested.

6: Wayfinding application

The wayfinding application stores some information in cookies to improve the user experience. The information stored in cookies includes the previous campus visited, language, and which version of the application was used last time use.mazemap.com was visited as well as information required by 10: Google Analytics.

7: Map Editor

The 7: Map Editor also uses cookies to a small degree. Some information tracking the map editing state is stored. This information includes campus ID, floor ID and similar that is related to the information that is being edited. Also, sessions are stored and the token used for authentication.

When a user logs in to the Map Editor, the user enters her password, which is hashed, and the the hash of the password entered by the user is compared to the hash stored in the cloud for that user. If the hash is the same, the user is authenticated and this information is stored in a session that is maintained by a session database. The session and a token are returned to the Map Editor. For every action the user makes, both the session and the token is sent to the server. Unless the user has done something for 15 minutes, the user must authenticate again.

8: LIPI server

The LIPI server is a server that runs behind the customer firewall. Its responsibility is to interface with the Cisco CMX/MSE so that the user's device that runs MazeMap can get the position from the CMX/MSE, as this is not supported directly by Cisco. No data is stored on the LIPI server unless the administrator turns on logging for debugging purposes. The LIPI servers are installed and administrated by the customers themselves.

9: Indoor positioning - Cisco CMX/MSE

Cisco CMX/MSE stores a position and the Mac address of the devices that are connected to the Wi-Fi network.Cisco CMX/MSE are behind the customers' firewalls and administered by the customer. MazeMap does not have or need access to Cisco CMX/MSE.

10: Google Analytics

Google Analytics collects information about the page visited (use.mazemap.com), the browser used and the user. The user information stored by Google is an approximate location derived from the IP address and language. MazeMap has no way of tracking this as Google Analytics only presents aggregated statistics to our administrators.

Personal data

MazeMap does not store the personal data of any users.