FAQ. Belimo Cloud Security & Privacy

How do I know that the product is secure?

Belimo's platform utilizes state-of-the-art security measures for data transmission, storage and access. Authentication and encryption are used for all communication via the Internet. The Belimo platform has undergone rigorous security testing. Multiple assessments have been conducted and are repeated periodically with external cyber security specialists.

Which security tests are performed on the Belimo cloud and cloud products?

- Black box hacking – a friendly hacker tries to hack the involved components without insider knowledge of the device or software and its security mechanisms
- System hardening – a friendly hacker analyzes the components with full knowledge and control of the device and/or software and proposes security improvements if needed
- System architecture review – hardware, software, production processes and infrastructure are all reviewed on a recurring basis

Does Belimo encrypt all data transmissions, including web server-to-server data transmissions?

Yes, all communication channels are authorized, encrypted and based on certificates with asymmetric keys; device to cloud, user to cloud, and cloud to cloud.

What security framework does Belimo utilize?

Belimo utilizes various frameworks and protocols including OAuth2, PKI, SSL, HTTPS.

What is my role in data protection and security?

Installation (see also connection guide):

- Make sure the device is installed in a Local Area Network (LAN) that is protected using enterprise-level security standards.
- The device must be able to connect to the internet, but may not in any case be accessible directly from the internet.

Passwords:

- Make sure you set distinct passwords for each device and your cloud account.
- Be diligent with protecting your passwords and cautious about distribution.

Privacy and Liability:

- When you connect a device to the cloud and have claimed it in your cloud account or cloud group, be sure that you have permission to manage this device from its legal owner and any possible third parties which use the facility in which it resides.

Where is the Belimo cloud located?

The Belimo cloud hosting and data storage is provided by Innofield AG, located in Switzerland. Innofield AG is FINMA (Swiss Financial Market Supervisory Authority) approved and ISO 27001 certified. Alternative cloud storage locations can be made available at the request of the customer.

What data is stored in the Belimo cloud?

The following data is stored:
The data from your cloud account, which is at minimum:

- Name
- E-mail address
- Job function
- Country

The data of the connected devices, which depends on the type of the device:

- Configuration data
- IP address of the Belimo device
- Product features and characteristics
- Product configuration (type of operation, target value, interface configuration)
- Software information (name, version, patch level)
- System condition values (system utilization and history)
- HVAC condition values (current sensor values, target values of actuators, information, warning and error reports)

Who can view data in the cloud?

Your cloud account data (name, e-mail, etc.) is only visible to you. A device's data is visible to cloud users who either have ownership of the device or have been granted access to the device by the owner. In addition, select Belimo employees have access to device data in order to provide services including but not limited to:

- Preparing and submitting service reports
- System optimization and efficiency increases
- Remote support for optimal configuration
- Support in cloud related questions and problems

Who owns the stored data?

A device's owner also owns the device's data and he has the right to access, download and delete this data. A data deletion request must be sent to Belimo.

Does Belimo keep a signed audit trail of users who have performed actions through the Belimo cloud?

Belimo maintains a traceable audit trail on each change made to a device. Audit trail logs are available in the cloud and can be accessed at any given time. Report logs are kept on file and can be retrieved at any given time. Changes made through standard Belimo cloud applications as well as 3rd party cloud applications using the client API will be tracked.

In the event of a data breach, what is Belimo's incident response process?

Belimo has an emergency and recovery plan in place in the event of a data breach. Whereas the roles, responsibilities, and actions for all parties (software supplier, infrastructure provider, Belimo support and developer) have been defined.

For more information please visit www.belimo.com/privacy