Häufig gestellte Fragen
Sicherheit und Datenschutz der Belimo Cloud

Woher weiss ich, ob das Produkt sicher ist?
Die Plattform von Belimo nutzt hochmoderne Sicherheitsmassnahmen für Datenübertragung, Speicherung und Zugriff. Für jede Kommunikation über das Internet wird eine Authentifizierung und Verschlüsselung verwendet. Die Belimo-Plattform wurde einer strengen Sicherheitsprüfung unterzogen. Verschiedene Sicherheitsbewertungen wurden durchgeführt und werden regelmässig mit externen Cyber Security-Spezialisten wiederholt.

Welche Sicherheits-Tests werden in der Belimo Cloud und mit den Cloud-Produkten durchgeführt?
- Black Box hacken – ein beauftragter Hacker versucht, in einzelne Komponenten ohne tiefere Kenntnisse über das Gerät oder Software und Sicherheitsmechanismen einzudringen
- System Hardening – ein beauftragter Hacker analysiert die Komponenten mit voller Kenntnis und Kontrolle über das Gerät und / oder die Software und schlägt bei Bedarf Sicherheitsverbesserungen vor
- System Architecture Review – verwendete Hardware, Software, Produktionsprozesse sowie Infrastruktur werden auf einer wiederkehrenden Basis überprüft

Verschlüsselt Belimo alle Datenübertragungen, einschliesslich «Webserver zu Server»-Datenübertragungen?
Ja, alle Kommunikationskanäle sind autorisiert und verschlüsselt auf Basis von Zertifikaten mit asymmetrischen Schlüsseln; Gerät zur Cloud, Benutzer zur Cloud und Cloud zu Cloud.

Welche Sicherheits-Frameworks nutzt Belimo?
Belimo verwendet verschiedene Frameworks und Protokolle, einschliesslich OAuth2, PKI, SSL und HTTPS.

Was ist meine Rolle bei Datenschutz und Datensicherheit?
Installation (siehe auch Connection Guide):
- Stellen Sie sicher, dass sich das Gerät in einem LAN (Local Area Network) befindet, das nach nach «State of the Art»-ICT-Sicherheit geschützt ist.
- Das Gerät muss sich mit dem Internet verbinden können. Es muss aber nicht zwingend vom Internet darauf zugegriffen werden können.
- Bei Geräten mit aktiver NFC-Funktion stellen sie sicher, dass Unberechtigte keinen physischen Zugang zum Gerät haben.

Passwörter:
- Stellen Sie sicher, dass Sie die Kennwörter für das Gerät und auch für Ihr Cloud-Konto nicht mehrfach verwenden.
- Seien Sie vorsichtig mit Ihren Passwörtern und mit wem Sie diese teilen.

Datenschutz und Haftung:
- Wenn Sie ein Gerät mit der Cloud verbinden und mit Ihrem Cloud-Konto verlinken, müssen Sie sicherstellen, dass Sie die Erlaubnis des rechtmässigen Eigentümers und möglicher Dritter, die die Anlage nutzen, bekommen.

Wo liegt die Belimo Cloud?
Das Belimo Cloud Hosting und die Datenspeicherung wird auf der Google Cloud Plattform (GCP) in Westeuropa administriert. Auf der GCP werden regelmässig Sicherheits-, Datenschutz- und Compliancekontrollen von unabhängigen Dritten durchgeführt.

Welche Daten sind in der Belimo Cloud gespeichert?
Gespeichert werden Daten aus Ihrem Cloud-Konto, also mindestens:
- Name
- E-Mail Adresse
- Funktion
- Land

Gespeichert werden zudem Daten der angeschlossenen Geräte, die abhängig sind von der Art des Geräts:
- Konfigurationsdaten
- IP-Adresse des Belimo-Geräts
- Produktmerkmale und Eigenschaften
- Produkt-Konfigurationen (Betriebsart, Werte, Schnittstellenkonfiguration)

- Software-Informationen (Name, Version, Patch-Level)
- Systemzustands-Werte (Systemauslastung und Historie)
- HLK-Betriebswerte (Aktuelle Sensor- und Antriebserte, Warn- und Fehlerberichte, sonstige Informationen)

Wer hat Zugang zu den Daten in der Cloud?

Die Daten Ihres Cloud-Kontos (Name, E-Mail, etc.) sind nur für Sie sichtbar. Die Gerätedaten sind nur für Benutzer sichtbar, die das Gerät besitzen, physischen Zugang zum Gerät mit aktivierter NFC Funktion haben, oder die vom Eigentümer die Zugriffs-Erlaubnis für ein Gerät erhalten haben. Zudem erhalten ausgewählte Belimo-Mitarbeiter Zugriff auf die Gerätedaten, um folgende Dienste zu gewährleisten (Liste der Dienste nicht abschliessend):

- Erstellung und Zustellung von Leistungsberichten
- Systemoptimierung und Effizienzsteigerung der Anlage
- Fernwartung zur optimalen Konfiguration des Gerätes
- Unterstützung bei Fragen und Problemen

Wem gehören die gespeicherten Daten?

Der Kunde besitzt die Daten und er hat das Recht auf den Zugriff, den Download und das Löschen seiner Daten. Für das Löschen von Daten, muss eine Lösch-Anforderung an Belimo gesendet werden.

Unterhält Belimo einen signierten Audit-Trail von Benutzern, die Aktionen durch die Belimo Cloud ausgeführt haben?

Belimo unterhält einen nachvollziehbaren Audit-Trail für jede Änderung am Gerät. Audit-Trail-Protokolle sind in der Cloud verfügbar und können jederzeit angefordert werden. Änderungen, die durch «Belimo Cloud»-Standardanwendungen oder durch Cloud-Anwendungen von Drittanbietern über die Client-API vorgenommen werden, werden ebenfalls verfolgt.

Wie ist im Falle eines Datenlecks das Verfahren der Belimo?

Belimo hat einen Notfall- und Wiederherstellungsplan für den Fall einer Verletzung der Datensicherheit. In diesem Verfahren sind die Rollen, Verantwortlichkeiten und Massnahmen für alle Beteiligten (Software-Anbieter, Infrastruktur-Unternehmen, Belimo-Support und -Entwicklung) genau definiert.

Mehr dazu erfahren Sie unter www.belimo.com/privacy