

# Mit uns sind Sie auf der sicheren Seite

Um Sie und Ihre Daten zu schützen, erfüllen wir und unsere Partner höchste Sicherheitsstandards, Vorschriften und Richtlinien. Für die sichere Datenübertragung nutzen wir aktuellste Verschlüsselungsverfahren und setzen auf aktuelle Sicherheitskonzepte und Standards bei der Authentifizierung und Autorisierung von SmartMonitoring. Zudem entwickeln wir nach dem „Security by Design“-Prinzip und unterziehen die Applikation regelmäßig einer Security-Analyse, um Sie und Ihre Daten vor Angreifern zu schützen. Es werden ausschließlich Daten verarbeitet, die für den Nutzen und den Zweck der Anwendung relevant sind. Ihre Privatsphäre ist uns wichtig, deswegen haben wir für Sie alle relevanten Informationen zusammengefasst. Sollten Sie darüber hinaus Fragen haben, kontaktieren Sie uns gerne unter [Produktinfo.lhv@liebherr.com](mailto:Produktinfo.lhv@liebherr.com)

## Was tun wir für Ihre Sicherheit?

### Eindeutige Kennung

Jeder Ihrer SmartCoolingHubs hat einen eindeutigen „Fingerabdruck“ und ist nur für Sie nutzbar. Nach einer geführten Einrichtung sind die Geräte eindeutig mit Ihrem Firmenaccount verbunden.

### Unterbrechungsfreie Versorgung

Bei Unterbrechung der Internetverbindung puffert jeder SmartCooling-Hub Messwerte bis zu 48h, um eine lückenlose Dokumentation zu gewährleisten. Zudem werden Sie über einen Verbindungsabbruch, ausgelöst durch ein lokales Netzwerk-Problem oder durch Ihr Internet, informiert und können umgehend handeln.

### Verschlüsselte Kommunikation

SmartCoolingHubs sind in alle gängigen LAN- und 2.4 GHz WLAN-Netzwerke integrierbar und kommunizieren verschlüsselt mit der SmartMonitoring Cloud.

### Regelmäßige Updates

Regelmäßige Updates halten Ihr System auf dem neusten Stand und sorgen für einen dauerhaft hohen Sicherheitsstandard.

### Berechtigungskonzept

Über das Rollenmanagement steuern Sie die Zugriffsrechte auf Ihr System und können darüber hinaus durch Einhaltung der Richtlinien zur Passwortsicherung Ihren Sicherheits-Beitrag leisten.

### Testings und Support

Um Ihnen eine ausgereifte Software mit einem langjährigen Support (LTS) zu gewährleisten, werden Änderungen in der Applikation im Vorfeld über mehrere Umgebungen ausgerollt, getestet und integriert.

### Security by Design

Die SmartMonitoring Applikation wurde nach den „Security by Design“-Prinzipien entwickelt und die Cyber-Physical-Security mit einem Team aus IoT-, Netzwerk-, Cloud- und Frontendspezialisten durchgeführt und protokolliert. Zudem stellen wir durch regelmäßige Updates sicher, dass wir z.B. veraltete Verschlüsselungsverfahren abschalten und die Anwendung auf dem aktuellen Stand der Technik halten. Dies schaffen wir durch kurze Update-Zyklen, die in der Form nur mit einer Cloud-Lösung möglich sind. Auf neue Erkenntnisse/Bedrohungen können wir sofort reagieren.

### Regelmäßige Scans

Regelmäßige Security-Scans erhöhen kontinuierlich die Leistung der gesamten Lösung. Erkannte Schwachstellen werden umgehend geschlossen und für künftige Updates evaluiert.

## Wie sicher sind Ihre Daten?

### Trennung von Nutzer- und Maschinendaten

Grundsätzlich separieren wir Benutzerdaten von Maschinendaten. Während die Telemetriedaten (z.B. Temperaturwerte) Ihrer Geräte in einem externen Rechenzentrum gespeichert werden, erfolgt die Speicherung Ihrer persönlichen Daten im eigenen Liebherr-Rechenzentrum in Deutschland.

### Externe Datenbank für Maschinendaten innerhalb der EU

Die Datenbank der Telemetriedaten nennen wir „SmartMonitoring Cloud“ und befindet sich in einem europäischen Rechenzentrum, welches diverse CSA STAR und ISO Zertifizierungen erfüllt. Das umfasst u.a. auch den ISO 27018 Standard für die Verarbeitung von Daten in der Cloud. Der Rechenzentrumsbetreiber stellt den professionellen Betrieb sicher und verfügt über umfangreiche technische und organisatorische Maßnahmen, um physikalischen Zugriff auf dessen Infrastruktur abzusichern.

### Datenschutz made in Europe

Wir nehmen den Schutz Ihrer Daten ernst und erfüllen die Regelungen zur DSGVO. In unseren Datenschutzhinweisen für SmartMonitoring haben wir für Sie hinterlegt, wer für die Verarbeitung Ihrer Daten verantwortlich ist, welche Daten zu welchem Zweck und auf welcher Rechtsgrundlage verarbeitet werden und wer die internen und externen Empfänger Ihrer Daten sind. Insgesamt halten wir uns bei der Beschreibung der Datenverarbeitung in SmartMonitoring streng an die Art. 13 / 14 der DSGVO. Die Datenschutzhinweise zu SmartMonitoring finden Sie im Download-Bereich.



Scannen und  
mehr erfahren.

# LIEBHERR