Datenschutz, Datenprivatheit und Datensicherheit bei der mobilen Sensorverwaltung von Hach

Der Datenschutz und die Datenprivatheit unserer Kunden ist ein Hauptanliegen von Hach®. Die Produkte, Entwicklungsprozesse und Verfahren von Hach entsprechen den international anerkannten Richtlinien zum Informationssicherheitsmanagement gemäß ISO/IEC 27001 sowie ISO/IEC 62443-4-1 und -4-2.

Ihre Daten sind geschützt.

Für jede Kommunikation zwischen der Hardware für Mobile Sensor Management und dem Remoteserver von Hach werden Secure Sockets Layer (SSL/TLS) Industriestandard-Verschlüsselungsalgorithmen mit 2048 Bit verwendet. Dadurch wird sichergestellt, dass nur bekannte und vertrauenswürdige Endpunkte miteinander kommunizieren können. Die installierten Firewalls gewährleisten, dass jeder sonstige Datenverkehr ignoriert wird. So können nicht autorisierte Dritte weder auf das System zugreifen noch die Datenkommunikation abhören.

Alle auf dem Server gespeicherten Daten (ruhende Daten) sind mithilfe aktuellster IT-Technologie und Betriebsprozesse verschlüsselt und gesichert.

Der Zugang zur Anwendung ist benutzernamen- und passwortgesteuert. Es wird nach dem Prinzip des kleinsten Privilegs (least privileged principle) sowie nach strengen Passwortrichtlinien verfahren, um zu gewährleisten, dass die Passwörter nicht erraten oder durch Brute-Force-Angriffe gefährdet werden.

Alle sensiblen Daten auf Geräten von Hach wie dem SC1500 oder dem DR3900 werden in einem „Datensafe" (verschlüsselter Flashspeicher) gespeichert. Dadurch sind die Daten auch dann geschützt, wenn die Geräte gestohlen werden und unautorisierte Dritte physischen Zugriff erlangen.

Ihre Daten sind privat.

Datenprivatheit bedeutet, dass nur Sie selbst und von Ihnen autorisierte Personen Ihre Daten einsehen können. Die Umsetzung von Hach ist nach einer der weltweit strengsten Datenschutzrichtlinien zertifiziert. Dies beinhaltet:

- Jegliches Schlüsselmaterial befindet sich ausschließlich im Besitz des Kunden.
- Die Kundendaten sind strikt getrennt.
- Lokale Server entsprechen den lokalen Richtlinien zur Datenprivatheit.
- Zugriff durch den technischen Support von Hach, über zertifikatbasierte VPN, erfolgt nur nach ausdrücklicher Aufforderung und Genehmigung durch den Kunden.
- Hach Administratoren melden sich mittels Zwei-Faktor-Authentifizierung im System des Mobile Sensor Management an.

Hach behält sich das Recht vor, die Daten zum Zweck der Produktentwicklung in anonymisierter Form abzufragen.

Ihre Daten sind sicher.

Die Verfügbarkeit des Remoteservers von Hach beträgt 99,9%. Das Datenzentrum führt alle Backups und Hot-Swaps bei Aufrüstung oder Ausfall der Hardware durch, sodass Sie immer auf Ihre Daten zugreifen können.

Die Daten werden auf mehreren Servern in verschiedenen Datenzentren gespeichert, sodass bei Bedarf eine schnelle Wiederherstellung der Daten gewährleistet ist.

- Zum Zweck der Notfallwiederherstellung befinden sich die Datenzentren an geografisch verschiedenen Standorten.

Um für Ihre Daten ein Höchstmaß an Sicherheit zu gewährleisten, hat Hach mit Microsoft einen professionellen, namhaften und sehr erfahrenen Partner gewonnen, dessen Expertise dem Schutz, der Privatheit und der Sicherheit Ihrer Daten dient. Weitere Informationen zur Konformität von Microsoft mit internationalen Vorschriften erhalten Sie unter: **https://azure.microsoft.com/en-us/support/trust-center/compliance**

Unten finden Sie eine Liste der wichtigsten Vorschriften und Richtlinien, die bei Hach Anwendung finden:

- IEC 62433 (international)
- ISO/IEC 27001-27005 (international)
- NIST 800-34, 800-53, 800-82 (international)
- BSI IT-Grundschutz (Deutschland)
- BDSG (Bundesdatenschutzgesetz, Deutschland)
- AWWA G340 (USA)

DOC063.72.30367.Nov16