

# Hach Mobile Sensor Management – datasikkerhed og beskyttelse af personlige oplysninger

Hos Hach® sætter vi kundernes datasikkerhed og beskyttelse af personlige oplysninger i forreste række. Hachs produkter, udviklingsprocesser og drift overholder de internationalt anerkendte retningslinjer for styring af informationssikkerhed, der er fastlagt i ISO/IEC 27001, ISO/IEC 62443-4-1 og -4-2.

## Dine data er beskyttet

Al kommunikation mellem Mobile Sensor Management hardware og Hachs eksterne server benytter industristandard 2048-bit Secure Sockets Layer (SSL/TLS) krypteringsalgoritmer, der sikrer, at kun kendte slutpunkter, der er tillid til, kan kommunikere. De implementerede firewalls sørger for, at al anden trafik ignoreres, så uautoriseret tredjepart ikke kan få adgang til systemet eller aflytte kommunikationen.

Alle data, der er gemt på serveren (data i hvile), krypteres og beskyttes ved hjælp af den nyeste it-teknologi og de nyeste driftsprocesser.

Adgang til programmet kontrolleres af brugernavn og adgangskode. Princippet om mindste privilegium håndhæves, og vi overholder strenge adgangskodepolitikker for at sikre, at ingen adgangskoder kan gættes eller kompromitteres ved hjælp af et brute force-angreb.

Alle følsomme data i Hach-enheder som SC1500 og DR 3900 gemmes i en "databoks" (krypteret flash-hukommelse). Herved opretholdes datasikkerheden, også selvom enhederne bliver stjålet, og uautoriseret tredjepart får fysisk adgang til dem.

## Dine data er private

Beskyttelse af personlige data betyder, at kun du og personer, du godkender, kan se dine data. Hachs implementering er certificeret i henhold til en af verdens mest restriktive politikker for databeskyttelse. Dette omfatter:

- Kunden er den eksklusive ejer af alt vigtigt materiale
- Streng adskillelse af kundens data
- Lokale regler for beskyttelse af data overholdes via lokale servere
- Hachs tekniske support får kun adgang via certifikatbaseret VPN efter kundens udtrykkelige invitation og godkendelse
- Hachs administratorer logger på Mobile Sensor Management-systemet via 2-faktor godkendelse

Hach forbeholder sig ret til at forespørge på data i anonymiseret form med henblik på produktudvikling.

## Dine data er sikre

Hachs eksterne server har en opetid på 99,9 %. Datacentret varetager alle sikkerhedskopier og serverskift ved hardwareopgradering eller hardwarefejl, så du altid har adgang til dine data.

Data gemmes på flere servere i forskellige datacentre, hvilket sikrer hurtig gendannelse af data, såfremt det er nødvendigt

- Datacentrene ligger på forskellige geografiske placeringer for genoprettelse i katastrofetilfælde

For at sikre den højeste grad af beskyttelse af dine data samarbejder Hach med Microsoft, som en professionel, anerkendt og meget erfaren ekspert, om at holde dine data beskyttet, private og sikre. Du kan finde yderligere oplysninger om Microsofts overholdelse af internationale regler under:

<https://azure.microsoft.com/en-us/support/trust-center/compliance>

Nedenfor finder du en oversigt over de vigtigste forordninger og direktiver, som Hach har anvendt:

- IEC 62433 (international)
- ISO/IEC 27001-27005 (international)
- NIST 800-34, 800-53, 800-82 (international)
- BSI it-beskyttelse (Tyskland)
- BDSG (BundesDatenSchutzGesetz, Tyskland)
- AWWA G340 (USA)