

# Sikkerhet i iBinder

## Datasentral

iBinder benytter Microsoft Azure som løsnings leverandør for vårt behov av datakraft (prosess) og lagringsplass. Avtalen tillater skalering av løsningen basert på behov (last). Microsoft Azure er ISO 27001 (Sertifisering for datasikkerhet) og ISO 27018 (Sertifisering for persondata) sertifisert. For ytterligere informasjon se:

<https://www.microsoft.com/en-us/trustcenter>.

## Tilgjengelighet og fysisk sikkerhet

Vi viser til: [https://www.microsoft.com/en-us/trustcenter/Security/AzureSecurity - Secure infrastructure](https://www.microsoft.com/en-us/trustcenter/Security/AzureSecurity-Secure_infrastructure), for beskrivelse av den fysiske sikkerheten.

## Taushetsplikt

Kunders passord gis ikke ut på telefon, men sendes via e-post til den adresse som kontoen er registrert på. Vår support legger ikke til deltagere eller endrer en deltagers rettigheter i et prosjekt uten tillatelse fra prosjektets administrator. Vår support gir ikke ut opplysninger om pågående prosjekt eller deltagere uten etter godkjenning fra prosjektets administrator. All inlogging til iBinder loggføres og kan spores ved behov. Opplasting av- eller fjerning av dokument loggføres og kan spores ved behov. Fire (4) personer hos iBinder har tilgang til systemets servere via VPN. Dette for å kunne utføre systemvedlikehold og sikre tilgjengelighet og funksjon på iBinder.

## Kommunikasjon

All kommunikasjon til og fra iBinder.com's servere kan skje med kryptert https-trafikk. For krypteringen benyttes 128 bits SSL. Anrop til serverne logges og kan spores ved behov.

## Driftsgaranti

Se våre allmene bestemmelser (General terms and Conditions) som finnes på [https://www.ibinder.com/pub/se/ibinder/pdf/iBinder General Terms and Conditions .pdf](https://www.ibinder.com/pub/se/ibinder/pdf/iBinder_General_Terms_and_Conditions.pdf)