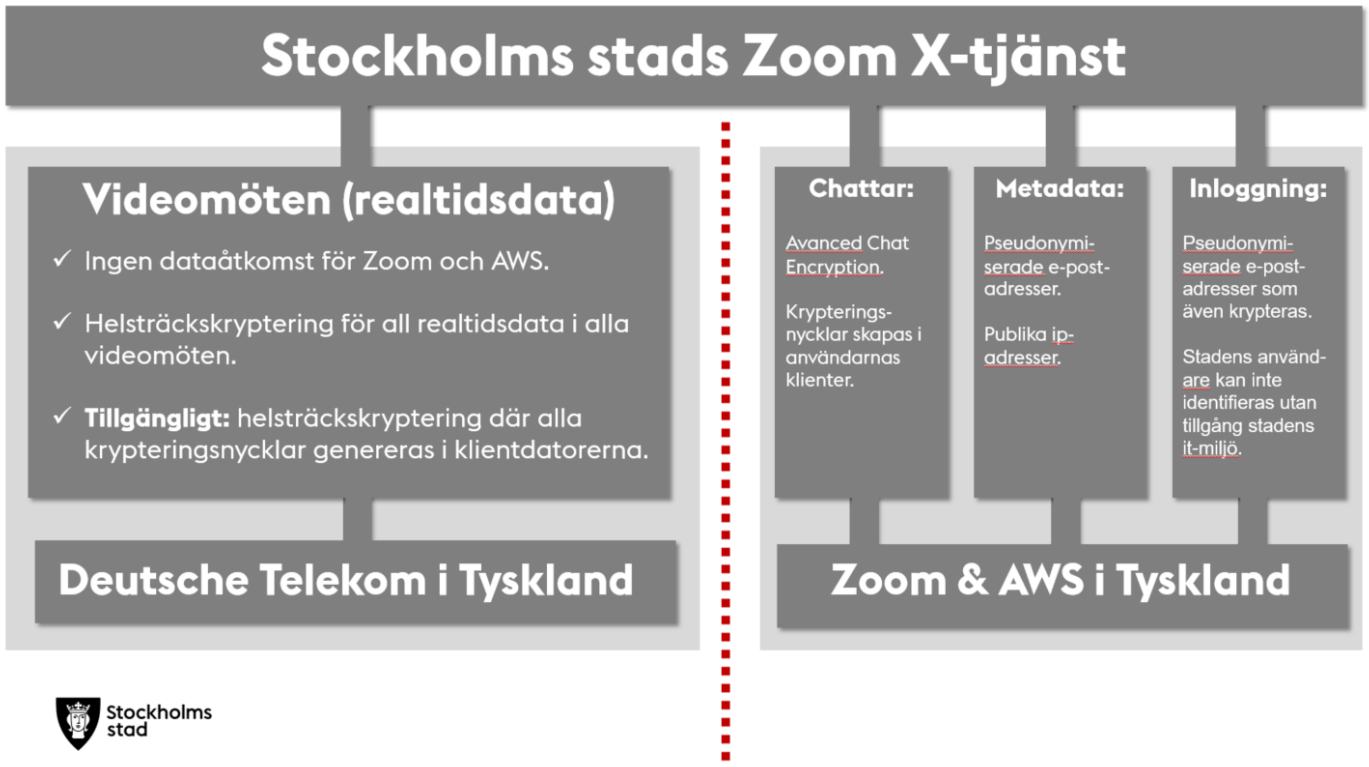
Säkerhet och personuppgiftshantering i Stockholms stads Zoom X-tjänst

Zoom X är ett av flera videomötesverktyg som används av Stockholms stad. Zoom X används för interna möten mellan medarbetare och även för vissa typer av videomöten med externa mötesdeltagare. Zoom X används inte för videomöten som hanterar känslig information och där det krävs att alla deltagares identitet säkras med e-legitimation. Här används istället videomötestjänsten Säkra digitala möten.

Videomöten oåtkomliga för amerikanska leverantörer

Driften av Stockholms stads Zoom X-tjänst hanteras av den tyska leverantören Deutsche Telekom fristående från amerikanska Zoom, vilket innebär att personuppgifter stannar inom EU. Staden har även infört ett flertal kompletterande skyddsåtgärder i Zoom X-tjänsten som säkerställer en korrekt personuppgiftshantering enligt GDPR.

Det innebär att all realtidsdata, exempelvis videomöten, inte är åtkomliga för Zoom och andra amerikanska leverantörer. Amerikanska myndigheter kan därför inte begära ut sådan data från tjänsten.



Kompletterande skyddsåtgärder

Realtidsdata:
All Realtidsdata i Stockholms stads Zoom X-tjänst är även krypterad mellan samtliga mötesdeltagares datorer och mobiler. I videomöten där alla deltagare använder Zoom X-appen är helsträckskryptering tillgänglig där alla krypteringsnycklar genereras i klientdatorerna.

Lagrad data (exempelvis metadata och textbaserade chattar):
Textbaserade chattar och metadata hanteras av Zoom och deras underleverantör AWS i deras it-miljöer i Tyskland, och kan därmed riskera att begäras ut av amerikanska myndigheter. Därför har Stockholms stad infört en rad kompletterande skyddsåtgärder:

- Chattmeddelanden skyddas med kryptering, Advanced Chat Encryption. Den fungerar så att krypteringsnycklarna genereras i chatt-deltagarnas programklienter. Krypteringsnycklarna är oåtkomliga

för Zoom och övriga leverantörer. Endast de användare som deltar i en chatt kan läsa meddelandena i klartext.

- När konton skapas i Zoom används en pseudonymiserad epost-adress. Det betyder att det inte går att identifiera användaren i Zoom utan tillgång till Stockholms stads it-miljö.

- Stockholms stad har begränsat antalet personattribut som skickas över till Zoom X när ett konto skapas till endast namn, pseudonymiserad e-postadress och organisationstillhörighet. Det innebär att amerikanska myndigheter inte med hjälp av metadata kan identifiera en användare. Endast namnuppgiften räcker inte i en amerikansk FISA-process för att säkert identifiera en användare då det kan finnas flera med samma namn.

- När användaren ansluter till tjänsten registreras den ip-adress som används som metadata av den amerikanska leverantören. Eftersom Stockholms stad använder publika ip-adresser, kan ingen förutom stadens egen internetleverantör veta vem som används vilken ip-adress vid ett givet tillfälle.

- Som en ytterligare skyddsåtgärd kommer också all metadata som kan kopplas till en person att raderas med jämna mellanrum. Även om en amerikansk myndighet skulle få tillgång till metadata, så sträcker tillgängligheten endast över kort tidsperiod.

Vi använder inte alla tillgängliga funktioner i Zoom X-tjänsten.

När det gäller några av Zoom X funktioner har Stockholms stad ännu inte infört tillräckliga skyddsåtgärder. Därför har dessa funktioner tillsvidare inte aktiverats i Stockholms stads Zoom X-tjänst *(se Ej beställda funktioner i bilden nedan)*.