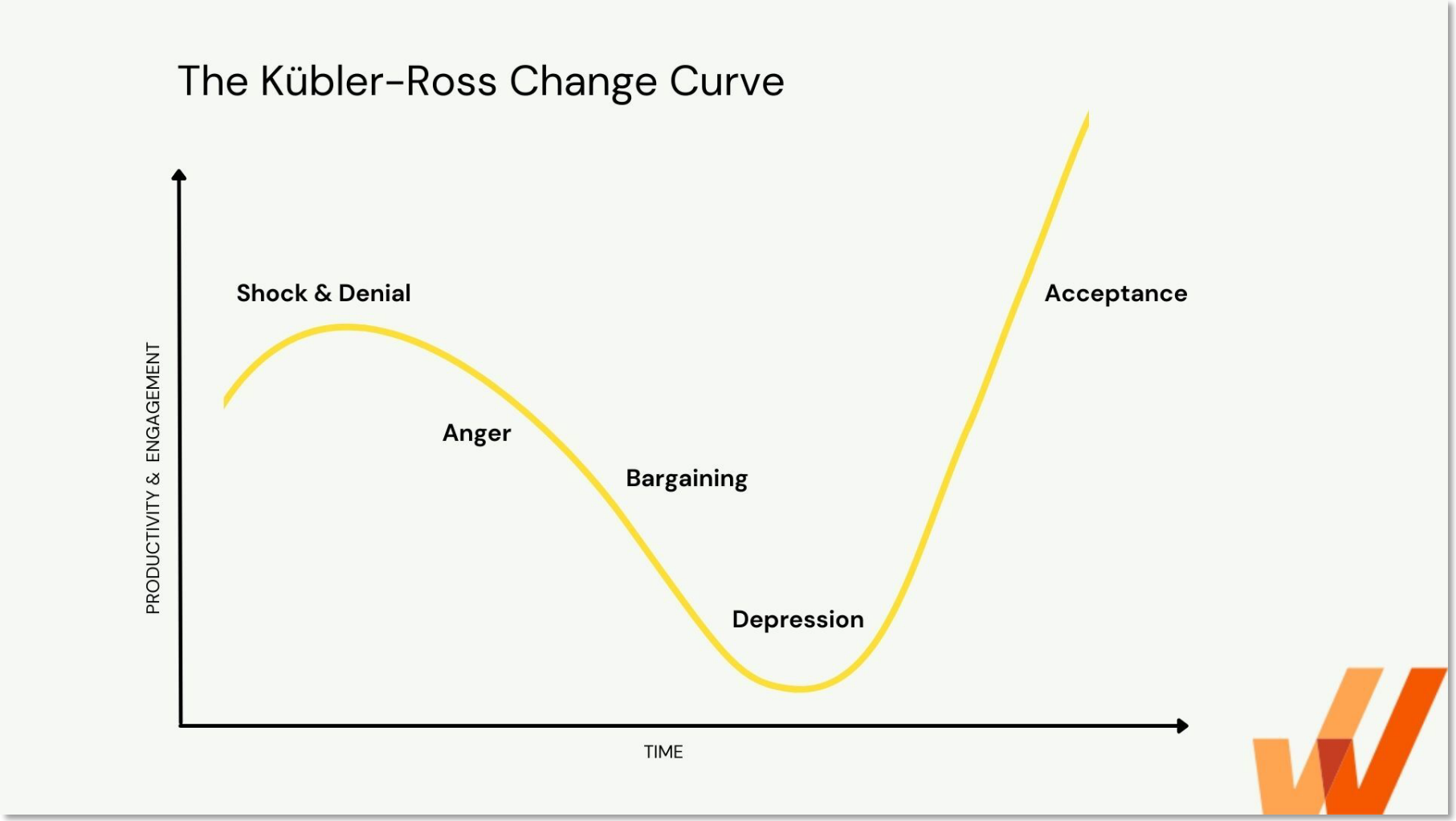
Stockholms stad och molnfrågan

Stockholms stad

Sambruk 221129
Anders Häregård

Schrems II: ”Som att förlora en nära vän”

- Förnekelse
- Ilska
- Förhandling
- Depression
- Acceptans



Stockholms stad

Sprida information och utreda

- Nyhet om Schrems II på intranätet publicerad den 14 september 2020
- Muntlig information till it-chefer, dataskyddsombud och kommunikationschefer via ordinarie kanaler
- Informationsbrev till nämnder och bolagsstyrelser med anledning av EU-domstolens dom i Schrems II-målet, utsänt 21 september 2020, Dnr KS 2020/1281
- Ny information på intranätssidan om dataskyddsförordningen och personuppgiftsbehandling
- Frågor och svar om Privacy Shield och Schrems II publicerade på intranätet
- Kartläggningsprocess och mallar framtagna
- Personuppgiftsansvariga är ansvariga för de tjänster man använder

Stockholms stad

Förhandssamråd om Teams med begränsad funktionalitet

- Stockholms stad ser ett stort behov av att komplettera de digitala mötesverktygen
- De bästa mötesverktygen idag levereras som molntjänster av amerikanska leverantörer
- Teams är enklast att implementera då staden redan har licenser för det
- Autentisering av användare i Teams sker via Azure AD, vilket förutsätter att personuppgifter i klartext synkroniseras från vårt on prem-AD till Azure AD
- Enligt Europeiska dataskyddsstyrelsen, EDPBs utkast till rekommendationer för tredjelandsöverföringar kan man inte överföra personuppgifter i klartext till tredjeland som inte når upp till likvärdig nivå av skydd för persondata som inom EU.

Stockholms stad

Integritetsskyddsmyndighetens bedömning

- IMY visar i sitt yttrande att de har förstått frågan och redovisar tydligt frågeställningen
- IMY anser att underlaget endast beskriver en begränsad del av behandlingen av personuppgifter, men ger ändå vägledning och råd
- Ett utlämnande till amerikanska myndigheter skulle kunna innebära att personuppgiftsbiträdet agerar i strid med såväl PUB-avtalet som dataskyddsförordningen.
- Staden behöver ta ställning till vilka garantier i form av tekniska och organisatoriska åtgärder som krävs. Om staden inte kan få tillräckliga garantier från ett avsett personuppgiftsbiträde, kan vi inte anlita det personuppgiftsbiträdet.
- Rättsläget är inte helt klart när det gäller frågan om vilka garantier och åtgärder från personuppgiftsbiträdet som skulle kunna vara tillräckliga i ett fall som det aktuella. EDPBs rekommendationer kan komma att förtydliga detta. De väntas antas under våren/sommaren

Konsekvenser av IMYs yttrande

- Den bedömning som tidigare kommunicerats till nämnder och bolag står fast, inga nya molntjänster som innebär tredjelandsöverföring av personuppgifter bör införas
- Om IMYs bedömning i yttrandet blir den gällande tolkningen skulle det innebära att alla molntjänster som har en överföring av personuppgifter i klartext till en amerikansk leverantör står i strid med Dataskyddsförordningen
- Detta skulle i så fall innebära att alla molntjänster som använder Azure AD och liknande tjänster för autentisering måste anpassas eller avvecklas
- Innan ytterligare beslut om åtgärder fattas kommer staden invänta att EDPBs rekommendationer blir klara

Stockholms stad

Stadens inriktningsbeslut dec 2021

1. Staden behåller nuvarande on prem-leverans för förvaltningar och bolag tills vidare. Inga nya molntjänster som innebär tredjelandsöverföringar av person-uppgifter i klartext till land utanför EU/EES eller till land som enligt EU-kommissionen inte uppnår adekvat skyddsnivå införs i den digitala arbetsplatsen.

Konsekvens:

Kräver ingen ny aktivitet på SLK IT, tas omhand inom förvaltningsobjekten

Stockholms stad

Stadens inriktningsbeslut dec 2021, forts

2. Avdelningen för it och digitalisering uppmanas att slutföra de införanden av kompletterande tjänster som påbörjats avseende säkra digitala möten och säkra meddelanden.
3. Med utgångspunkt i identifierade behov bör de ekonomiska och organisatoriska förutsättningarna för införande av ytterligare kompletterande tjänster i den digitala arbetsplatsen för förvaltningar och bolag utredas. I de fall där ett införande är möjligt genomförs förändringen lämpligen genom ändringar i befintliga avtal med leverantörer.

Konsekvens:

- VP-aktivitet för 2022:
  Avdelningen ska, utifrån beslutad molnutredning, utreda och om möjligt införa kompletterande digitala samarbetsverktyg samt slutföra införandet av säkra digitala möten och meddelanden.

Stockholms stad

Stadens inriktningsbeslut dec 2021, forts

4. De personuppgiftsansvariga, framför allt inom de pedagogiska verksamheterna, som idag använder molntjänster och där det inte går att införa kompletterande skyddsåtgärder som innebär att personuppgiftsbiträdet kan ge tillräckliga garantier för en lagenlig personuppgiftshantering rekommenderas att senast inför nästa licensperiod finna alternativ som uppfyller lagstadgade krav. Utbildningsförvaltningen uppmanas att ta fram en plan för åtgärder och redovisa den för styrgruppen för informationssäkerhet senast 2022-03-30.

Konsekvens:

- Ansvaret för att följa upp arbetet med att säkerställa en lagenlig personuppgiftshantering i verksamheterna ligger i linjen.

  Förvaltningsobjektet för informationssäkerhet följer upp plan och åtgärder.

Stockholms stad

Stadens inriktningsbeslut dec 2021, forts

5. Även hanteringen av mobila enheter som t ex smartphones, användande av internet och sociala medier och deltagande i andra organisationers samarbetsplattformar behöver analyseras närmare med avseende på tredjelands-överföringar. Om problem identifieras ska införande av skyddsåtgärder eller byte till tjänster som uppfyller kraven genomföras så långt det är möjligt utan att verksamheternas förmåga att genomföra sina uppdrag försämras.

Konsekvens:

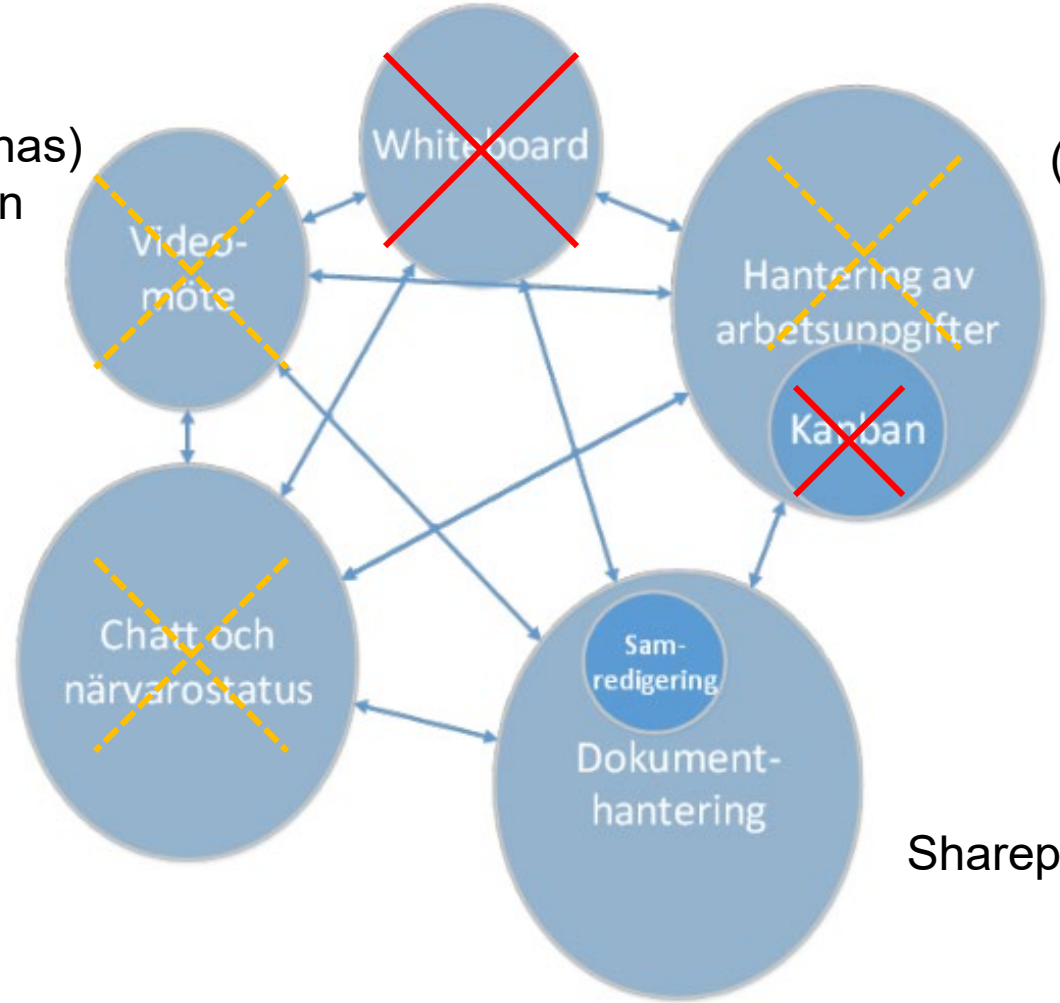
- Ansvaret för att tjänsterna uppfyller kraven på informationssäkerhet ligger i linjen.

  Respektive förvaltningsobjekt ansvarar för att utreda och vidta åtgärder.

Stockholms stad

Nuläge i den digitala arbetsplatsen

Skype (funktioner saknas)
Säkra digitala möten



(Sharepoint)

Skype
(endast möteschatt)

Sharepoint

Stockholms stad

Effektmål

Användare av den digitala arbetsplatsen för förvaltningar och bolag upplever att de har tillgång till effektiva mötes- och samarbetsverktyg för att utföra sitt arbete.

Stockholms stad

Två huvudspår under våren

Compliant Collaboration

- Tjänst som levereras av Tietoevry on prem
- Bygger på dSams kravlista och matchning
- Stor möjlighet att påverka hur lösningen ser ut, staden kan få sina krav tillgodosedda
- Nytt för Tietoevry att inte jobba med Microsoftprodukter, viss erfarenhet finns i Finland
- Verktygens funktioner testade av en referensgrupp

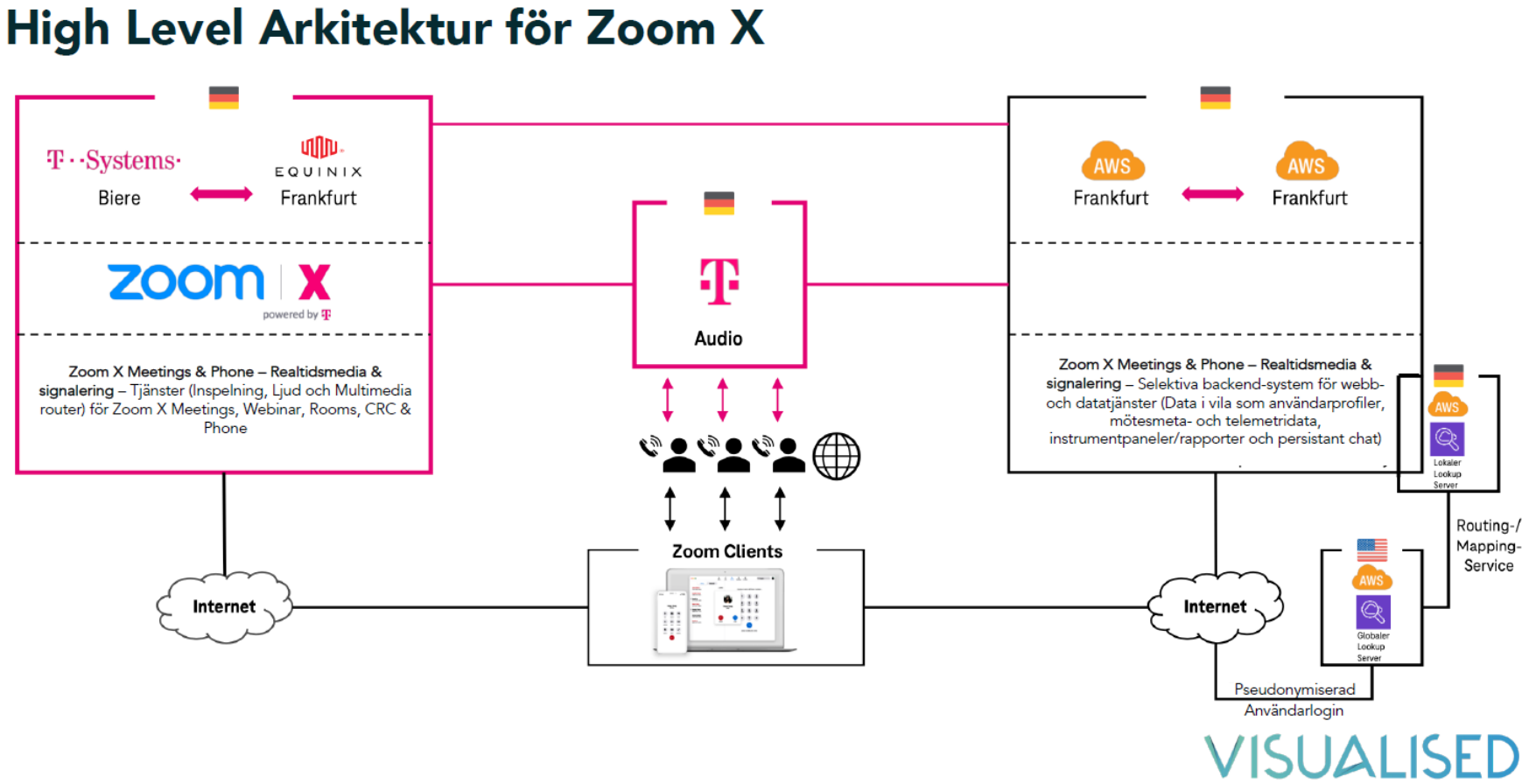
Zoom med pseudonymisering

- Installeras on prem och driftas av Tietoevry
- Tjänsten kräver inloggning på amerikansk server med ett fåtal användaruppgifter (namn, e-postadress)
- Användaruppgifter pseudonymiseras innan de skickas till Zoom
- TIA genomförd och godkänd av DSO om tillräcklig nivå på pseudonymisering och kryptering används

Stockholms stad

Allt pekade på Tietoevry…

- …men så i sista stund:



Stockholms stad

Vad är möjligt att göra med en amerikansk leverantör?

Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

Version 2.0

Adopted on 18 June 2021

Stockholms stad

EDPBs metod för Transfer Impact Assessment

1. Know your transfers
2. Identify the transfer tools you are relying on
3. Assess whether the Article 46 GDPR transfer tool you are relying on is effective in light of all circumstances of the transfer
4. Adopt supplementary measures
5. Procedural steps if you have identified effective supplementary measures
6. Re-evaluate at appropriate intervals

Stockholms stad

Transfer Impact Assessment
Steg 1: Know your transfers

	A	B	C	D	E	F	G	H	
	Transfer Impact Assessment Data Sheet		**Assessment of ZoomX powered by DT, provided by Visualised AB.**		**The first line is a summary impact assessment for personal data. The remaining lines break down the data categories and sub categories for assessment**				
	No	**Category/ sub-category**	**Processing purpose**	**Data content**	**Data Subject**	**Sensitive personal data**	**Processing Location**	**Controller / Processor / Subprocessor**	**Access**
4	12	**Account data - end user** **According to ref A.** **This is data at rest**	Account Data (end-user): This is information associated with end users of a Zoom Enterprise or Education account. Depending on how the account administrator has configured the Zoom Enterprise or Education account, this information includes the data content listed. External participants may also participate without account via their browser, as guest.	Account Data (end-user): This is information associated with end users of a Zoom Enterprise or Education account. Depending on how the account administrator has configured the Zoom Enterprise or Education account, this information includes: • Zoom unique user ID, • Social media login (optional) • Profile picture (optional), • Display name, and • Customer authentication data unless Single Sign On ("SSO") is used. According to ref A.	Account Data (end-user): This is information associated with end users of a Zoom Enterprise or Education account. Depending on how the account administrator has configured the Zoom Enterprise or Education account, this information includes: • Zoom unique user ID, • Social media login (optional) • Profile picture (optional), • Display name, and +J14:L14 According to ref A.	Account Data does not contain information meeting the defintion of Sensitive Personal Data found in Article 9 of the GDPR.	Data is stored at AWS data centers in Germany	Controller - Stockholms Stad Processor- Visualised Subprocessor - DT DT uses subprocessors, see: Amendment 3 to the agreement between Zoom and DT	Zoom and su physically acc Access to any tightly controll Data are encr
5	13	**Account holder business data** **According to 2.** **This is data at rest**	Account Holder Business Data: This is information associated with the individual(s) who are the sales contact for a Zoom Enterprise or Education account for provisioning and registering an account, includes the data content listed.	• Name • Address • Phone number • Email address • Data related to the Customer's account, such as subscription plan and selected controls. According to ref A.	Zoom X account holders	Account Data does not contain information meeting the defintion of Sensitive Personal Data found in Article 9 of the GDPR.	Billing is handled by Swedish reseller Visualised AB and subprocessor DT	Controller - Stockholms Stad Processor- Visualised Subprocessor - DT DT uses subprocessors, see: Amendment 3 to the agreement between Zoom and DT	Zoom does s name, compa email domair registration a purposes in t
6	14	**Support data** **According to ref A.** **This is data at rest**	Ability to ask Visualised for Support with issues when using the Zoom service 'Meetings'	• Tier 1 + 2: Support is provided by the processor • In the case of Tier 3, support is provided by the subprocessor. The support ticket may contain personal data.	Employees of Stockholms Stad who are provisioned with a Zoom account and any meeting participants invited to a videoconference or call by such an employee of Stockholm Stad.	Support Data has no need to contain information meeting the defintion of Sensitive Personal Data found in Article 9 of the GDPR. Support data could includ sensitive personal data	1st and 2nd line support is processed by Visualised AB and stored in Sweden.	Controller - Stockholms Stad Processor- Visualised Subprocessor - DT DT uses subprocessors, see: Amendment 3 to the agreement between Zoom and DT	Zoom and su access to dat support case consults to Vi information)
	15	**Feedback data**	Feedback data is information about end users' satisfaction with Zoom	Optional (not activated by default)	Employees of Stockholms Stad	Feedback Data does not contain information	Data is stored at AWS data	Controller - Stockholms Stad	Zoom and su

Stockholms stad

Nästa steg

- Beslut om budget för 2023 tas 13 december
- Tester visar positiva resultat
- Utrullning påbörjas i början av året

Stockholms stad