TRAFIKVERKET

**REMM** – resfria/digitala möten i myndigheter

# Molnfrågan och digitala möten
## – möjliga vägar för myndigheter framåt

Under en workshop som genomfördes av REMM tillsammans med eSam och DIGG den 24 april 2020 belystes tre frågeställningar i ämnet "myndigheters möjlighet till att använda molnbaserade tjänster för digitala möten":

1. Vad ska utredas/kartläggas och vem gör vad?
2. Tillämpningar som införts i samband med Corona hur ser vi på detta?
3. Möjliga vägar framåt?

Syftet med workshopen var att tillsammans diskutera ämnet eftersom många upplever en stor otydlighet i om det är okej att för egen del använda molnbaserade tjänster.

Frågorna användes som diskussionsstöd. Tid gavs inte att gå in på djupet på alla frågeställningar. I detta dokument finns en övergripande sammanfattning.

Trafikverket driver sedan 2011 projektet REMM – resfria/digitala möten i myndigheter. REMM startade som ett regringsuppdrag 2011–2015 och samordnar arbetet inom ett antal utpekade statliga myndigheter med att bli bättre på att byta vanliga möten mellan och inom myndigheterna mot digitala möten. remm.se



Ulf Pilerot
Trafikverket
Proj.led. REMM
010-123 75 42
ulf.pilerot@trafikverket.se


Per Schillander
Trafikverket
Bitr. proj.led. REMM
010-123 59 85
per.schillander@trafikverket.se


Thonita Hellgren
Trafikverket
Projektstöd REMM
010-123 35 68
tonita.hellgren@trafikverket.se


Peter Björk
Trafikverket
Projektstöd REMM
0738-83 41 88
peter.bjork@trafikverket.se


Peter Arnfalk,
Lunds universitet/
Arnfalk Consulting
Expertstöd REMM
070-522 21 33
peter.arnfalk@remm.se


Selene Samuelsson
Hedlund, EcoBonum
Expertstöd REMM
0708-38 00 05
selene.samuelsson.hedlund@remm.se


Pontus Grönvall
Stormen kommunikation
Expertstöd REMM
0705-67 37 47
pontus.gronvall@remm.se

# Tillägg om personuppgifter (Schrems II)

Efter REMMs workshop i april 2020 har det kommit en EU-dom i fallet Schrems II. Denna dom förtydligar vad som juridiskt sett påverkar svenska myndigheter gällande personuppgifter och hur de får hanteras av leverantörer vars IT-tjänster faller under så kallad tredjelands juristriktion.

Varje myndighet och verksamhet måste göra sin egen bedömning. Men Schrems II-domen pekar tydligt på två saker gällande amerikanska leverantörers hantering av kunds personuppgifter kopplat till lagar de måste följa (till exempel GDPR kontra Cloud Act):

- Europiska kunder har inte fullgott skydd enligt våra lagar för personuppgifter kopplat till ”Privacy Shield” (gällande omedelbart).
- EU har avtal framtagna vilka skulle kunna användas för att tillräckligt skydda dessa affärer, men grundförutsättningarna i amerikansk domstol saknas för att kunna införliva dessa extra avtal (om amerikanska leverantörer skulle godkänna dessa avtal).

Detta rör dels rätten att bli informerad om hur sin personuppgift hanteras, dels rätten att få hantera saken som EU-medlem i amerikansk domstol (vilka man ej har). Tvärtom finns amerikansk lag som hårt bötfäller amerikanska leverantörer om dessa på eget bevåg (utan specifikt tillstånd) informerar kund om personuppgift hämtats ut/använts.

Tydligt gör denna dom det svårare för EU att nyttja molntjänster (som ägs av till exempel amerikanska företag) så som Slack, MS Teams och Zoom. Men exakt vad detta landar i är inte helt lätt att bedöma. Domen har dessutom skapat diverse febril motreaktion, till exempel har arbete påbörjats av ny uppdaterad ”Privacy Shield”-avtal EU–USA (kan ta några år att få på plats), flera molnleverantörer börjar testa/införa molntjänster vilka ej synkas EU–USA (spelar det någon roll?). USA är tydliga med att deras lagar står fast. Så en naturlig strategi, beroende på hur tillsynsmyndigheten Datainspektionen väljer att agera, är att avvakta. Speciellt om man som myndighet ej redan har skaffat denna typ av molnleverantör/tjänst.

De flesta stora myndigheter i Sverige har nu tagit fram eller tar fram en intern organisation för att se över alla gjorda upphandlingar (med en IT-leverans) för myndigheterna. Hittar man ”privacy shield”-baserade affärer rivs dessa upphandlingar upp och görs om.

Enligt svensk lag måste varje organisation göra en egen bedömning. Med i denna bedömning finns också myndighetens möjlighet att utföra sitt myndighetsuppdrag (alla aspekter måste betänkas). Se över hur en exitplan och ersättningslösning kan se ut (då detta tar tid om detta blir relevant). Sedan lär man behöva ta ett beslut med stöd av myndighetens ledning i hur att agera på kort och lång sikt runt frågan. Betänk också att domen berör alla molnleveranser inte bara specifikt mötestekniker.

# 1: Vad ska utredas/kartläggas och vem gör vad?

Vad behöver respektive myndighet själva kartlägga för att kunna tillämpa befintliga och kommande riktlinjer? Vad kan/borde utredas gemensamt – och av vem? Informationsklassificering samt matcha informationsklassning med säkerhetsklassning av mötestjänster? Vilka lagar gäller? Krav på digitala mötestjänster från verksamheten i olika situationer?

## Gemensamma riktlinjer

Myndigheterna inom REMM ser ett stort och akut behov av gemensamma standarder, ramverk och riktlinjer för digitala mötestjänster, framförallt vad det gäller molnbaserade lösningar. Lyfts vidare till lämplig arbetsgrupp att utforma.

**Förslag:**

- Lyfts vidare till lämplig arbetsgrupp att utforma.
- Även eSam bör utforma, med stöd av andra specialister inom området.

## Klassning och hantering av information samt personuppgifter

Myndigheterna har kommit olika långt i frågan om klassificering av information, och hur väl spridd denna kunskap är bland personalen.

### Olika modeller, definitioner och skalor

Det finns olika klassningsmodeller, definitioner och skalor inom informationssäkerhet. Vad är eller kan vara gemensamt och vad skiljer sig mellan myndigheters olika modeller? Läs mer på dessa länkar:

- www.informationssakerhet.se/metodstodet/anvanda/#klassningsmodell
- www.informationssakerhet.se/siteassets/metodstod-for-lis/1.-om-metodstodet/vagledning-utforma-klassningsmodell_kommentarsperiod.pdf
- www.sakerhetspolisen.se/download/18.7acd465e16b4e0e54c673/1560952186689/Vagledning-Informationssakerhet.pdf

Modellerna bygger på matriser som är olika komplexa beroende på om man hanterar säkerhetsskyddsklassificerade uppgifter eller inte. Matriserna kan variera mellan två och fem nivåer, där den sistnämnda innefattar säkerhetsskydd som är tillagt ovanpå för särskild hantering. Olika myndigheter har utifrån detta gjort egna lokala tolkningar av MSBs vägledning/förordning. Till exempel har Trafikverket utöver dessa dimensioner lagt till spårbarhet.

### Nödvändigt eller bara ett hjälpmedel?

Flera av REMMs myndigheter ställer sig frågan: Är säkerhetsklassning  nödvändigt eller bara ett hjälpmedel för att få till en likriktning eller enkel mappning/översättning mellan olika myndigheter?

Ett exempel på när enhetlig säkerhetsklassning behövs är i de fall där myndigheterna samarbetar och ska dela information med varandra. Är det lätt och självklart att avgöra vem som äger informationen som ska delas? Vi vill ju inte riskera att bedömningen hos myndighet A klassas på en viss nivå men hanteras annorlunda hos myndighet B.

**Förslag:**

- Ta fram några typfall. Görs av ansvariga för processen ”hantera information” hos några av REMMs större myndigheter. Här finns stöd och vägledning: www.esamverka.se/stod-och-vagledning.html

**Kan och får vi dela med oss av modellerna och hur gör vi det isåfall?**

Informationsklassificering behöver genomföras och kunskapen om detta måste spridas till all personal, då det är de som i slutändan hanterar informationen. Det kan finnas ett behov av att ha gemensamma diskussioner och lärande av varandra för att lyckas med frågan.

**Förslag:**

- Låt eSAM förtydliga hur myndigheters modeller kring informationsklassning ser ut och hur modellerna kan översättas för att bli kompatibla, där det är möjligt.

Varje lösning behöver genomgå en analys och klassificering, för att bedöma till vilken nivå som lösningen går att använda.

Detta åligger varje myndighet att driva och genomföra. Vid högre nivåer, som innefattar säkerhetsskyddsklassificerade uppgifter, ska detta samrådas, läs mer om detta här:

- www.sakerhetspolisen.se/download/18.7acd465e16b4e0e54c673/1560952186689/Vagledning-Informationssakerhet.pdf

I dokumentet i länken ovan står bland annat:

- *”Vid ett sådant samråd lämnar Säkerhetspolisen ett yttrande kring de säkerhetsskyddsåtgärder verksamhetsutövaren har vidtagit, eller har för avsikt att vidta, samt hur dessa förhåller sig till bestämmelserna om säkerhetsskydd i författningarna.”*
- *”Av bestämmelserna i 3 kap. 2 § säkerhetsskyddsförordningen (2018:658) framgår att: 2 §: Innan ett informationssystem som kan förutses komma att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre tas i drift, eller i väsentliga avseenden förändras, ska verksamhetsutövaren skriftligen samråda med Säkerhetspolisen. Om verksamhetsutövaren hör till Försvarsmaktens tillsynsområde enligt 7 kap. 1 § första stycket 1, ska denne i stället samråda med Försvarsmakten. Samrådsskyldigheten gäller även i fråga om andra informationssystem än sådana som anges i första stycket, om obehörig åtkomst till systemen kan medföra en skada för Sveriges säkerhet som inte är obetydlig.”*

**Förslag:**

- Det kan finnas ett behov av att ha gemensamma diskussioner och lärande av varandra för att lyckas med frågan. Till exempel myndighetssamarbete REMM och REDI samt temamöten, som REMM anordnar för sina medlemmar.

| Säkerhetsskyddsklass | Den skada som ett röjande av uppgifterna kan medföra | Värdeord till stöd för bedömningen om en viss typ av skada föreligger |
|---|---|---|
| Kvalificerat hemlig | Ett röjande kan medföra en synnerligen allvarlig skada. | Synnerligen allvarliga negativa konsekvenser av stor omfattning, under lång tid, som utgör ett direkt hot mot den nationella förmågan. Konsekvenserna är inte begränsade till enstaka funktioner. Mycket svårt att återställa. |
| Hemlig | Ett röjande kan medföra en allvarlig skada. | Allvarliga/betydande negativa konsekvenser, av stor omfattning eller av väsentlig art, som innebär ett direkt hot mot den nationella förmågan, om än mot avgränsade funktioner. Svårt att återställa. |
| Konfidentiell | Ett röjande kan medföra en inte obetydlig skada. | Påtagliga negativa konsekvenser för den nationella förmågan, om än i begränsad omfattning, som äventyrar, vållar skada, hindrar, underlättar för en antagonist eller innebär större avbrott. |
| Begränsat hemlig | Ett röjande kan medföra endast ringa skada. | Ringa negativa konsekvenser som är begränsade till att påverka, försvåra eller störa den nationella förmågan i mindre omfattning. |

*Vägledning för indelning i säkerhetsskyddsklass. Säkerhetsskyddsklassificerade uppgifter ska delas in i säkerhetsskyddsklasser utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet. Källa: Vägledning i säkerhetsskydd - Informationssäkerhet, Säkerhetspolisen, juni 2019.*

## Vad säger eSam?

eSam är ett medlemsdrivet program för samverkan mellan 27 myndigheter och SKR. Medlemmarna vill ta tillvara digitaliseringens möjligheter för att underlätta för privatpersoner och företag och för att använda gemensamma resurser på ett effektivt sätt. eSam anser att man ska likställa köp av molnbaserade digitala mötestjänster med outsourcing:

- https://esamverka.se/nyheter/nyheter/2020-05-26-kommentar-till-kritisk-rapport-om-molntjanster-i-offentlig-sektor.html (ny information som tillkommit efter vår workshop)

Samma rapport pekar också ut att myndighetsinformation i dessa molntjänster måste anses som röjd information *”om det inte är osannolikt att leverantören tar del av uppgifterna eller lämnar ut dem till någon annan”*. Vilket man allmänt anser att det är.

Detta öppnar för till exempel ”end-to-end”-kryptering (vid skapande, vid nyttjande, under transport, vid lagring, vid backup, vid avveckling) eller där molntjänsten levereras som container och privat molnlösning (men kan fortsatt vara en korrekt sourcad IT-leverans, det vill säga betrodd tredje part). Utgångspunkten är att ingen leverantör ska kunna ge sig själva otillåten access till myndighetens information som huvudadministratör för den tekniska tjänsten. Svaret på om detta är en möjlig väg för viss myndighet och viss molntjänst tas fram i den lösningens analysfas, med de expertkompetenser inom området som myndigheten har till förfogande (kan röra sig om inhyrda expertiskonsulter). Det måste bli så då de tekniska förutsättningarna per molntjänst (eller per myndighet) aldrig är helt samma, samt att dessa tekniska förutsättningar ändras löpande av leverantören via inkrementella ändringar av molntjänsten.

## Skiljer det sig med vem man kan dela information med på en högre informationsklass?

Svenska lagar för hantering och utlämning av information pekar ej ut *”pålitliga” eller ”opålitliga”* motparter (leverantörer/andra myndigheter) utan handlar till exempel vid utlämning av allmän handling om alla motparter. Det kan dock finns framtagna samarbetssätt mellan myndigheter, till exempel via SGSI (myndighets kommunikationsnätverk) eller tekniska systemintegrationer. Dessutom kan delning av viss information mellan myndigheter innebära krav på diarieföring och andra typer av krav.

Just nu vet vi att länder som har ”cloud act”-liknande lagstiftning får en särställning vid utlämning av svensk myndighetsinformation, då dessa länder ger sig själva rätten att fritt hämta all information från kunderna till alla IT-bolag som är skrivna i landet (och dess dotterbolag). Därmed och enligt eSams bedömning är all denna information i dessa ”cloud act”-molntjänster röjd.

Vad som är personuppgifter tolkas på olika sätt och detta är ett stort problem. För att kunna ansluta till molnbaserade digitala mötestjänster så behöver vissa personliga uppgifter skapas i molntjänsten.

**Förslag:**

- Datainspektionen tar en tydligare roll att klargöra vad som ska anses som känsliga personuppgifter, så att myndigheterna får en samsyn i frågan.
- Slå samman krav mot molntjänster baserat på myndighetstyp, till exempel alla i totalförsvaret (med beredskap), alla som har krisberedskap och alla som berörs av NIS. Till dessa grupper (och ev ytterligare grupper) kan specifika krav kopplas (vilka övriga myndigheter kan ignorera). MSB bör ha en samlad bild över vilka legala krav som ställs på respektive myndighet.

---

Observera att beskrivningen om EU-domen Schrems II (se ovan) tydligt beskriver en ny problemställning, som inte var känd vid REMMs workshop den 24/4-2020, och som har företräde i tolkning.

# 2: Tillämpningar som införts i samband med Corona?

Har molnlösningar använts och hur väl har de fungerat? Flera har upplevt att det kraftigt ökade behovet av digitala möten i samband med Corona innebär att man frångår regelverk och använder de lösningar man tycker fungerar bäst, till exempel Teams och Zoom.

Universitet och högskolor använder Zoom genom Sunet, kopplad till NORDUnet. Denna lösning är helt skild från den publika molnbaserade lösningen. Användningen har ökat kraftigt, men det har fungerat bra. Myndigheter utanför universitets- och högskolesfären använder också Zoom, men då den publika molnbaserade lösningen.

Zoom har ökat sin användning från tio miljoner användare till 300 miljoner användare på några månader. Zoom har kritiserats för säkerhetsbrister och har den senaste tiden kommit med en rad säkerhetsuppdateringar. Om uppmärksamheten kring och åtgärder för att komma till rätta med säkerhetsbrister leder till att Zoom blir väl så säkert eller kanske ännu säkrare alternativ återstår att se.

När man har forskningskontakter med andra universitet runt om i världen behöver man vara med på det projektets premisser.

Myndigheter ska samarbete, men har olika plattformar. Är det rimligt att säga att myndigheterna ska ha bara en lösning?

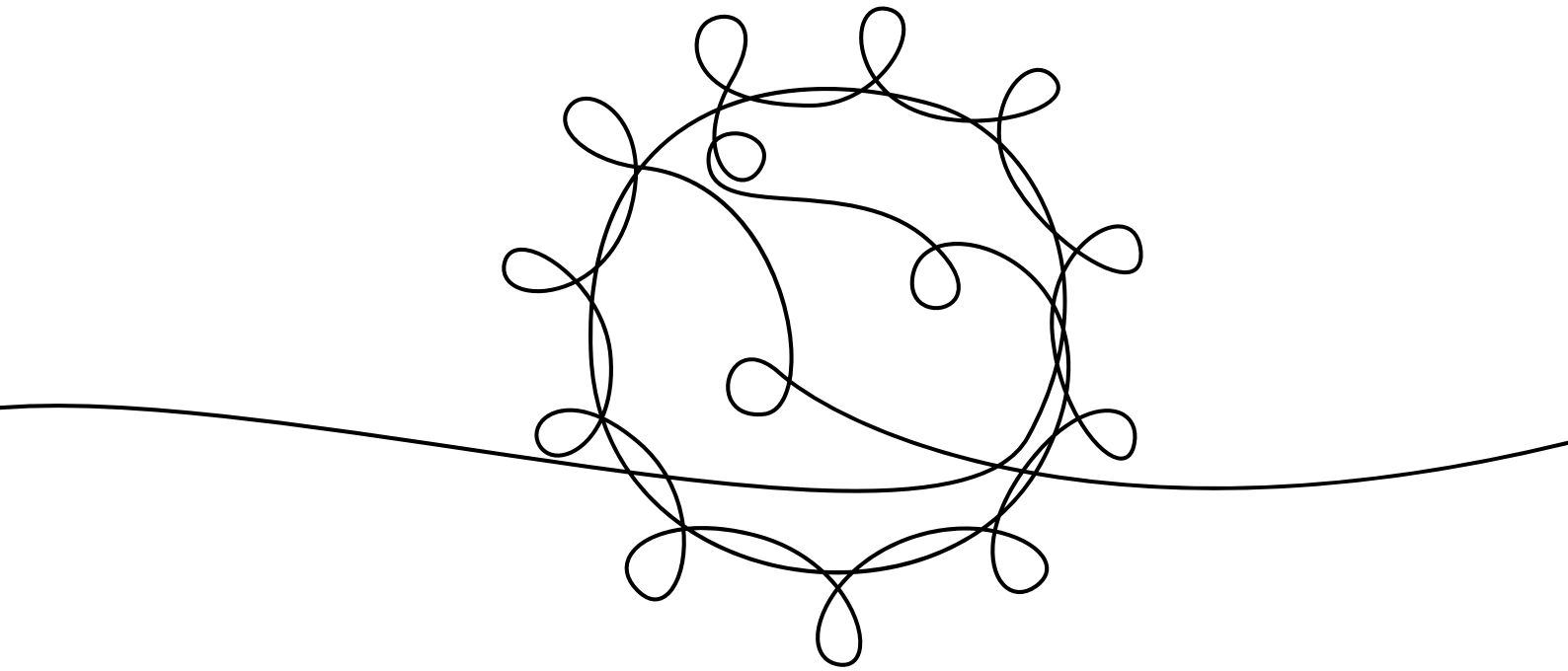
### Kan man behålla dessa eller måste man backa?

Följande diskuterades:

- Det är problematiskt att inte regeringen kan bistå med riktlinjer, i förhållande till Cloud Act. Någon kommenterade att juridiska tolkningen blir som teologin, man söker efter stöd som verifierar vad man bestämt sig för att tro på.
- All känslig information ska lagras internt, men det är svårt att hantera, liknar e-post. Ingen frågar om e-post. Varför resonerar vi olika beroende på vilken tjänst vi talar om, eller vilken leverantör det gäller? Ibland blir det lite ”sila mygg och svälja kameler”.

---

Observera att beskrivningen om EU-domen Schrems II (se ovan) tydligt beskriver en ny problemställning, som inte var känd vid REMMs workshop den 24/4-2020, och som har företräde i tolkning.



# 3: Möjliga vägar framåt?

Möjligheten av att använda flera digitala mötestjänster parallellt hos en myndighet? Alternativet att köra vidare på on-prem lösningar – hur ser utvecklingsstrategierna ut hos de större tillverkarna? Kort och lång sikt? Andra lösningar – vilka kan dessa vara och vad krävs för att realisera dem?

## Rekommenderat arbetssätt för myndigheter

Utifrån en sjufrågorsprincip, där varje fråga ska hanteras tillräckligt:

1. Stark marknadsanalys. Vilka stora och små lösningar finns på marknaden? Vilka är cloud only? Vilka är on prem? Vilka tillåter privat cloud, till exempel containerteknik? Vilka av dessa publika moln lyder under Cloud Act-liknande lagar?
2. Vilka informationsklasser kommer myndigheten någon gång att behöva exponera i tjänsten? Finns det en chans att av misstag lagra fel information (till exempel en för hög informationsklass) i tjänsten?
3. Kan myndigheten hantera alla behov av informationsklass med tredjepart-verktyg, till exempel CASB, DLP, EDRM och Information governance? Löser myndigheten även hantering av till exempel personuppgift? Går dessa tekniska lösningarna att kringgå?
4. Kan vi hantera alla behov av informationsklass med framtagna, enkla, manuella arbetsrutiner?
5. Har myndigheten rätt kompetens och rätt resurser för att klara av att hantera detta även under beredskap?
6. Möter tänkta lösningar alla övriga myndighetenskrav (arkivering, diariehantering, fyrstegsprincip, gallring, informationssäkerhet, it-driftkrav, olika strategier och så vidare)?
7. Med alla dessa förutsättningar plus att molntjänster snabbt kan ändras över tid, samt att lagar ändras, är planerad väg fortfarande ett stark affärscase och en sund långsiktig strategi för myndigheten?

Detta kan leda till att vissa myndigheter behöver se olika tekniska lösningar för olika informationsklasser. Vissa eller alla av dessa lösningar kan vara en molntjänst, men då troligtvis via privata kontrollerade moln för säkerhetsskyddad information.

---

Observera att beskrivningen om EU-domen Schrems II (se ovan) tydligt beskriver en ny problemställning, som inte var känd vid REMMs workshop den 24/4-2020, och som har företräde i tolkning.


**Säkra digitala möten**

**Säkerhetsskyddat information**
- Inom skalskydd
- Vissa nät
- Vissa klienter

**Teknikförslag**
- Cisco Meeting
- Next Cloud
- Pexip

**Digitala möten - internt**

**För lägre informationsklass**
- Med omvärlden
- Kontortelefon
- Status

**Teknikförslag**
- Skype for Business

**Digital konferans**

**För öppen information**
- Avlyssning spelar ingen roll
- Ingen teknisk koppling till Trafikverket

**Teknikförslag**
- Google Meet
- Gotomeeting
- MS Teams
- Slack
- Webex
- Zoom

**Digitala möten - andras**

**Omvärldens egna mötesplattformar**
Hur skyddar myndigheter sin information från tex informationsdelning eller personuppgifter?

**Teknikförslag**
- Agentlöst deltagande och med spärr på filutbyte via webb
- Paketera alla vanliga kända mötesklientprogramvaror

*Denna bild kan ge en känsla för hur man kan tänka som myndighet kring digitala möten, exempel från Trafikverket.*