Myndigheters Möten i Molnet 2.0

Sammanfattning chatt **webbinarium** 2021-01-29

Myndigheters möten i molnet (MMiM) är en oerhört aktuell fråga, inte minst på grund av Corona-pandemin. Den 29 januari 2021 fortsatte diskussionen inom REMM om huruvida myndigheter får och bör använda sig av molnbaserade digitala mötestjänster. Förmiddagen startade med ett webbinarium och följdes sedan av en workshop. Aktiviteten var en fortsättning på diskussioner som startade den 24 april 2020.

I webbinariet deltog cirka 250 personer. Inspelning och dokumentation från webbinariet finns här på remm.se.

Nedan redovisas en sammanfattning av frågor och diskussion från chatten, som inte lyftes muntligt under webbinariet. **Observera att detta är frågor och kommentarer från anonyma deltagare som speglar hur debatten gick och är inte ställningstagande från REMM.**

- Vad är Schrems II?
- Schrems II – snabbsammanfattning: att använda identifierbara personuppgifter i tjänster som är kopplade till USA är inte tillåtet. Och en massa annat.
- Jag kan rekommendera nyhetsbrevet från techlaw.se som går igenom händelser efter Schrems II.
- Schrems II (Privacy Shields demise) gör ingen skillnad på kategorin av personuppgifter. Däremot kan ju t.ex. eventuella konsekvenser påverkas utifrån vilken sorts information det är. Känsliga personuppgifter i USA innan Schrems II gås igenom ganska detaljerat i IMY:s sanktionsbeslut mot Umeå universitet.
- Som jag uppfattar det så handlar det i huvudsak om amerikanska myndigheters rätt att kräva ut data från amerikanska företags moln. Vad gäller företags möjlighet att sälja data vidare så bör det kunna regleras i avtal. Eller?
- Ska man hårddra detta försvårar Schrems II även användning av lokalt installerade program då man ofta måste registrera sig (med jobb-epost) för att få tillgång till licensnyckeln eller att programmet ”ringer hem” för att kontrollera om det finns uppdateringar mm. Rimligt?
- Sen hör man sällan någon problematisering kring nivån på personuppgifter. Det måste rimligtvis vara skillnad på min jobb-epostadress och min sjukjournal. Skulle gärna höra ett resonemang om detta och hur detta påverkas av Schremsdomen

- Finns det någon som tittat närmare på Signal? https://signal.org

- Universiteten kör Zoom OnPrem i egna servrar på egna kommunikationsnät
- Den tillämpning av Zoom som nordiska universitet använder är inte den publika tjänst som vem som helst kan använda utan en helt separat installation inom NORDUnet. NORDUnet är en sammanslutning mellan universitetsdatanätverken i de fem nordiska länderna, däribland svenska SUNET. Den fysiska installationen ligger helt och hållet i de nordiska länderna och det gäller även den molntjänst som upphandlats som förstärkning. Installationen

är GDPR-säkrad och personuppgifter lagras inom EU. NORDUnet ansvarar för avtalet med Zoom och bevakar att regler och riktlinjer följs.
- Vi diskuterar med Zooms svenska leverantör Visualised om att sätta upp Zoom OnPrem på egna servrar på myndigheten. Dom erbjuder den formen av leverans idag.
- NORDUnets Zoom hanterar personuppgifter i servrar som lyder under amerikansk lagstiftning. Servrar i EU, men amerikansk lagstiftning FISA702 är extraterritoriell och gäller även Zooms servrar i EU. Dvs i praktiken överföring till tredje land.
- Zoom som företag kan se en begränsad del av personuppgifter i NORDUnets Zoom. De kan inte se någon som helst mötesdata. Men visst detta måste bevakas. Det finns ingen ren ”on-prem” av zoom, det är en hybrid där metadata om möten om personuppgifter om deltagare hanteras i molnet och därmed exponeras mot USA.

- Att man har behov av säkra möten är en sak men i detta är frågan hur stor del av mötena som behöver vara säkra av totalen är också viktigt. Säkra möten jämfört med konfidentiella möten borde vara frågan.
- En viktig aspekt att ta hänsyn till är vi som behöver ha digitala möten med motpart som inte är myndighet (annan offentlig sektor eller privat företag) men där vi behandlar känsliga personuppgifter
- Det borde gå att skilja mellan relativt ”harmlösa” personuppgifter som e-postadress som borde kräva lägre ”skyddsnivå” än mer känsliga personuppgifter? Går det inte att kryptera just de känsliga personuppgifterna? Att de då kan lämnas ut, men bara ses som ettor och nollor, men inte går att förstå?
- Det finns inget begrepp som heter ”personuppgifter av ringa betydelse” i GDPR. Det finns särskilt skyddsvärda (ex personnummer, ekonomisk information m.m.) och särskilda kategorier (hälsa, sexuell läggning, etnicitet m.m.)
- Men är det inte så att vi nämner betydelsen av informationsklassning men i resonemanget så bortser vi ifrån det och vill hantera allt utifrån vår högsta klassning. Det känns ju inte konstruktivt.

- Om svenska staten förhandlar fram ett PUB-avtal med Microsoft för myndigheters räkning och säkerställer där att personuppgifter INTE får föras över – är det en lösning? Staten och Microsoft kan inte avtala bort amerikansk lagstiftning.
- Det har framkommit, EU-domstolen EDPB, att Microsoft lämnar personuppgifter till minst 6 andra bolag i samband med inloggning från MS-appar i mobila enheter.

- Tillgänglighet i molntjänster måste idag betraktas som hög, men om en myndighet bygger verksamheten i ”molnet”. Hur blir tillgängligheten i ett krisläge?
- Lösning för många myndigheter är att anställda skaffa privat konton i en massa onlinetjänster för att kunna arbeta.

- Är det rimligt att lägga detta ansvar på varje myndighet? Det finns myndigheter som är runt 20 personer.
- Någon statlig myndighet som MSB borde få utreda det här grundligt och komma med riktlinjer. Vansinne att myndigheter ska slösa skattemedel på att utreda detta på var sitt håll med hänvisning till myndigheters självbestämmande. Räcker ju med en enveten jurist eller personuppgiftsansvarig för att stoppa allt. Vi bryter samtidigt mot lagen om vi inte kan utföra våra uppgifter.
- DIGG har fått uppdrag att ge rättsligt stöd i digitaliseringsfrågor.

- En utmaning är ju att interoperabiliteten och standardiseringen för att kunna ansluta mellan t.ex. olika mötestjänster brister. Någon som vet om det bedrivs någon form av strategiskt standardiseringsarbete som kan ge effekt på det området?
- Vi har idag stora svårigheter att delta på internationella möten digitalt och rösta bl.a. Det får stora konsekvenser på sikt på våra möjligheter att påverka.

- Det skulle vara mycket intressant att hitta tjänster UTAN överföring till 3:e land. Någon som har/vet??

- Medborgarperspektivet – videomöten – ingår det i analysen?

- Sen har vi ju elefanten i rummet, E-post. hur resonerar vi kring användning av detta? Visst händer det att det krypteras ibland men vad jag förstå är det inte regel nästan någonstans. Har ni ett resonemang om detta?
- Fler elefanter: VISA/Mastercard mfl, telefoni, världsövergripande flygbiljetts-system, mm, mm.

- European data protection Board – Övergripande sammanslutning av tillsynsmyndigheterna, inte EU-domstolen: https://edpb.europa.eu

- Europa ligger långt efter USA och Kina med att tillhandahålla molntjänster. Vad jag förstår är inte statliga aktörer dessa leverantörers största och viktigaste kunder. Inte alls säkert att de anpassar sig utifrån våra behov i Europa. Vad händer nu också med Brexit efter övergångsperioden?

- IP-adress leder till en dator leder till en användare = personuppgift. Det borde stoppa all användning av Internet. Är det i så fall GDPR som är felskriven?

- EU borde förhandla för alla medlemsländers myndigheter.

- Någon som kikat på nextcloud? https://nextcloud.com/enterprise/ SUNET håller på att lansera en tjänst, SUNET Drive som bygger på nextcloud

- Länk till eSam:s nyligen publicerade promemoria om tekniska förutsättningar i molntjänster:
  - https://www.esamverka.se/aktuellt/nyheter/nyheter/2021-01-28-tekniska-forutsattningar-i-molntjanster.html
  - https://www.esamverka.se/download/18.2592ea441774291f4c756db/1611825241932/PM%20Teknik%20och%20molntjänster%201.0%202021.pdf

/Version 210312, Pontus Grönvall, REMM