

Juridiska frågeställningar som bör utredas för bättre och säkrare digitala möten

December 14, 2017

Trafikverkets projekt REMM – resfria/digitala möten i myndigheter

Projektledare Ulf Pilerot, Trafikverket/REMM-gruppen, 010-123 75 42,
ulf.pilerot@trafikverket.se

Expertstöd Peter Arnfalk, REMM-gruppen, 070-522 21 33, peter.arnfalk@remm.se

Inledning

Digitala möten är en viktig del i det genomgripande digitaliseringsarbete som pågår i svenska myndigheter. Trafikverket och REMM¹ vill därför göra den pågående utredningen ”Rättsliga förutsättningar för en digitalt samverkande förvaltning” uppmärksam på ett antal rättsliga frågeställningar som bör klargöras och besvaras för att skapa förutsättningar och underlätta användningen av digitala möten och samverkan i våra myndigheter. Detta dokument baseras på samlade erfarenheter från REMMs 82 myndigheter och från konferenser och webinarier som REMM arrangerat runt dessa frågor. Frågeställningarna nedan är exempel på vanliga frågeställningar och de är listade utan någon inbördes rangordning.

Förslag till åtgärder

1. Ta fram en vägledning som kan besvara frågor nedan.
2. Utöver en vägledning bör checklistor och rutiner utvecklas gemensamt.
3. Myndigheterna bör få tillgång till en central stödfunktion som de kan vända sig till och konsultera i dessa frågor.

Hantering av inspelningar av möten, webinarier och konferenser

En stor osäkerhet råder bland myndigheter om vad som gäller för inspelning av möten, webinarier och konferenser (hädanefter kallade ”möten”), och hur man ska hantera det inspelade materialet. Riksarkivet håller just nu på att ta fram myndighetsspecifika föreskrifter för universitet och högskolor (U&H) om gallring och annan arkivhantering. Utöver dessa så är de enda riktlinjer som vi har känner till de som återfinns i ”Legala handboken 2.0 – en guide för lärare och studenter i Internetdjungeln” (2014).

Vad ska man tänka på innan och när man spelar in?

- I vilka fall får man, bör man och när får/bör man *inte* spela in ett möte?
- Måste man meddela i början av ett möte att detta kommer att spelas in?
- Måste/bör detta göras redan vid kallelsen/inbjudan till mötet?
- Kan en deltagare förhindra att mötet spelas in, krävs det samtycke?
- Bör/måste man redovisa hur det inspelade materialet kommer att hanteras och spridas?
- Måste man spara exempelvis chatten eller kan man välja att inte spara den?

Hantering av sparad material?

- Vem äger materialet, vem får nyttja det?
- Får man lägga ut en allmänt tillgänglig länk till inspelningen?
- Behöver det lagras och i så fall hur länge?
- Hur och var ska inspelningar av möten lagras?
- Får/bör man använda molntjänster, och får dessa tjänster i så fall hanteras av tjänsteleverantörer utanför Europa?
- När kan/bör/måste det inspelade materialet gallras ut?

¹ 2011 fick Trafikverket regeringens uppdrag att vara ett stöd för att öka andelen resfria/digitala möten och har sedan dess drivit projektet REMM – resfria/digitala möten i myndigheter. REMM samordnar arbetet inom ett antal av regeringen utvalda myndigheter. Under perioden 2011–2015 skedde samordningen för 20 myndigheter och 2016 fick ytterligare 62 myndigheter i uppdrag i sina regleringsbrev att arbeta enligt REMMs metod.

Vad är offentlig allmän handling?

- I vilka fall är en inspelning av ett möte, som har arrangerats av en myndighet, att betrakta som offentlig allmän handling? I vilka fall är det inte det? Exempelvis behandlar vissa myndigheter inspelningarna som arbetshandlingar/anteckningar, vilka i sin tur leder till andra dokument som man då diarieför. En inspelning av ett möte i en projektgrupp raderas därför skyndsamt. Men inspelningar av möten/föreläsningar som kommer att visas externt blir då också normalt offentliga.
- Sekretess – vilka möjligheter har myndigheter att INTE lämna ut redan inspelat material?

Hantering av möten mellan tjänsteman och medborgare kund

- Får webbkamera användas då handläggare på en myndighet möter medborgare eller sina ”kunder”?²
- Hur hantera incidenter såsom då handläggning via video spelats in av ”kund” och lagts upp på Facebook efteråt?
- Vilka möjligheter finns att använda video vid t.ex. tolkning och vittnesförhör?
- I vilka fall ska/bör man kräva att deltagarna identifierar sig? T.ex. Försäkringskassan skiljer på ”inloggade” och ”oinloggade” möten.

Informationssäkerhet och personlig integritet

- Vilka uppgifter får man inte avhandla över webb/video? Ex. personuppgifter, andra konfidentiella uppgifter?
- Ska skärmdelning, filöverföring och *presence* (dvs man kan se om någon är inloggad) tillåtas i webbmöten på myndighet i allmänhet eller i det specifika fallet, för ett visst möte?
- Bör myndigheter med höga säkerhetskrav informationsklassa digitala möten och hantera dessa därefter? Alternativt komplettera/anpassa existerande rutiner för fysiska möten till digitala möten.

Autentisering

- Om en myndighetsperson pratar med/intervjuar en person/medborgare, hur vet man då att hen är hen? Hur ska personerna identifiera sig? Kanske BankID³, Swamid⁴ som för U&H, eller SITHS⁵ som är vanligt för e-hälsa?
- Bör man alltid identifiera sig i digitala möten med myndigheter, även mellan myndighetspersoner?

² Försäkringskassan erbjuder i vissa fall sina kunder att träffa en handläggare vid ett webbmöte man kallar ”det personliga digitala mötet”. Datainspektionen har beslutat att man inte får använda webbkameras vid dessa möten, men Försäkringskassan har överklagat till Förvaltningsrätten och så länge Datainspektionens föreläggande inte har vunnit laga kraft kommer videosamtal fortsatt kunna erbjudas som en del i ett personligt webbmöte.

³ Skatteuppglysningen testade under hösten 2015 identifiering i telefon via Mobilt BankID, vilket ger utökade möjligheter till fördjupad information om medborgarens specifika ärende. Försöket har slagit mycket väl ut och kommer att börja erbjudas i större utsträckning.

⁴ SWAMID är en identitetsfederation som omfattar de flesta lärosäten, forskningsinstitut och andra myndigheter som är relaterade till svensk forsknings- och utbildningssektor. SWAMID drivs av SUNET. <https://www.sunet.se/swamid/>

⁵ Identifieringstjänst SITHS är en säkerhetslösning som gör det möjligt för användare att identifiera sig med stark autentisering vid inloggning i e-tjänster. SITHS kan också användas för kryptering av information när e-tjänster, system eller servrar kommunicerar med varandra. SITHS-kortet har många användningsområden och är en av de viktigaste grundtjänsterna inom nationell e-hälsa.

Diskussion

En del av dessa frågeställningar kan sannolikt hanteras genom rekommendationer av REMM, i form av en enkel vägledning, kompletterat av rekommendationer från SUNET⁶ för frågor som är specifika för relevanta högre lärosäten. De skulle i så fall baseras på REMM-myndigheters utarbetade praxis och erfarenhet i frågan. REMM bör i så fall få i uppdrag att ta fram sådana rekommendationer, samt de resurser som skulle krävas för arbetet.

Men för vissa frågor bör juridisk expertis anlitas för att bland annat inte äventyra myndigheterna säkerhet eller medarbetarnas eller medborgares personliga integritet.

Utöver dessa ovan identifierade hinder och frågeställningar, så erbjuder digitala möten även möjligheten att utveckla myndighetsarbetet i Sverige och göra det mer demokratiskt och jämställt. REMMs vision är att den digitala tillgängligheten även ska innefatta olika former av möten och att svenska myndigheter får i uppdrag att erbjuda sina anställda denna möjlighet.

Visionen om digital tillgänglighet till möten, seminarier och konferenser i det offentliga Sverige

Sverige ska vara världsledande inom digital samverkan i offentlig verksamhet. Alla myndighetsanställda ska kunna kalla till och delta i digitala möten.

Att kunna delta i möten, seminarier och konferenser oberoende var man befinner dig i landet och vilka fysiska och ekonomiska möjligheter människor har att förflytta sig, är en viktig demokrati- och jämlikhetsfråga.

Vision:

- Alla myndigheter kan erbjuda bra digitala alternativ för tillgång till seminarier och konferenser, där det är befogat.
- Alla anställda i statliga myndigheter kan be om att få bli digitalt uppkopplade vid möten i tjänsten, där detta är möjligt och befogat.
- I båda dessa fall bör Regeringskansliet visa vägen och utgöra ett gott exempel.

För att nå visionen krävs en rad insatser på många plan, inklusive de tre åtgärder som föreslås början av i detta dokument.

⁶ SUNET står för Swedish University computer Network och har i uppgift att skapa infrastruktur för nationell och internationell datakommunikation på universitet, högskolor och andra anslutna organisationer.