Datum
2014-10-14

Diarienr
2014-3403-2

Ert datum
2014-07-03

Er referens
N2014/2822/ITP

Verksamhetsstöd
Rättsenheten
Per-Olof Wikström
010-240 5293
per-olof.wikstrom@msb.se

Regeringskansliet
Näringsdepartementet
103 33 Stockholm

Så enkelt som möjligt för så många som möjligt – Bättre juridiska förutsättningar för samverkan och service (SOU 2014:39)

Sammanfattande synpunkter

Myndigheten för samhällsskydd och beredskap (MSB) har mottagit ovan angiven utredning på remiss. I remissen presenterar E-delegationen sitt förslag på hur e-förvaltningen kan utvecklas och bygger detta på en extensiv tolkning av undantagsregeln i tryckfrihetsförordningens 2 kap. 10 §.

MSB ser positivt på en utveckling av effektiv, säker och långsiktigt hållbar e-förvaltning. En sådan utveckling måste dock vila på en solid rättslig grund samt använda sig av lösningar som uppfyller krav på integritetsskydd och informationssäkerhet. En utveckling som inte på ett tillräckligt sätt har beaktat detta riskerar att, till och med på kort varsel, behöva stängas ned eller förändras i grunden i det fall den rättsliga grunden eller de säkerhetsmässiga förutsättningarna befinns otillräckliga. Konsekvenserna, både avseende ekonomiska förluster och förlorat förtroende hos allmänheten och näringslivet, kan bli avsevärda.

MSB ser inte att delegationen på ett övertygande sätt, med nödvändigt stöd i rättskällorna, har visat att den föreslagna extensiva tolkningen av undantagsregeln i tryckfrihetsförordningen är så rättsligt hållbar att den kan läggas till grund för ett omfattande och resurskrävande utvecklingsarbete på e-förvaltningsområdet. Förutsebarheten är starkt begränsad. MSB ser inte heller att delegationen i sina analyser har beaktat skyddet av integritet och informationssäkerhetsaspekter i tillräcklig utsträckning, vilket öppnar för allvarliga brister i dessa avseenden. Förslaget ger även mycket lite ledning för hur detta praktiskt ska användas hos statliga och kommunala myndigheter, vilka ska få ett ”eget utrymme”, hur ska personuppgiftsansvaret kunna utövas etc.

MSB har inte bara invändningar mot den presenterade lösningen utan har även, för att visa på möjligheterna på området, tagit fram förslag på ett alternativt rättsligt upplägg som följer grundlagens huvudregler samt gör det

möjligt att skapa de förutsättningar för skydd av information som krävs för att hantera uppgifter i offentlig verksamhet. Förslaget ger samma möjligheter att utveckla e-förvaltning som delegationens förslag. Bakgrunden till att MSB tagit fram förslaget är att myndigheten är starkt tveksam till E-delegationens inställning att det för en utveckling av e-förvaltningen är nödvändigt att finna en lösning där uppgifter undanhålls från den grundlagsreglerade hanteringen av allmänna handlingar. Denna inställning motiveras företrädesvis med att vissa aktörer känner sig ”obekväma” med att inskickade handlingar blir allmänna eftersom det öppnar upp för viss hantering från myndighetens sida. Det av MSB redovisade förslaget visar att det finns goda möjligheter att hantera aktörernas önskemål och behov på annat sätt än att markant utvidga tillämpningsområdet för ett av de få undantagen från reglerna om handlingsoffentlighet som vi har i grundlagen. Det är inte acceptabelt att vissa aktörers känsla av att det är obekvämt att följa offentlighetsprincipens huvudregler ska styra utvecklingen inom e-förvaltningsområdet. Mot bakgrund av bristerna efterfrågar MSB en djupare analys av olika alternativa lösningar, detta saknas i betänkandet.

Utgångspunkter

MSB har i sin instruktion uppdraget att samordna och stödja samhällets arbete med informationssäkerhet och remissvaret har utformats utifrån MSB:s uppdrag varför både rättsliga och informationssäkerhetsmässiga aspekter behandlas.

Med informationssäkerhet avses att omge informationen med rätt nivå av skydd i aspekterna konfidentialitet, riktighet, spårbarhet och tillgänglighet. Att säkerställa tillräcklig nivå av skydd kring information och informations-hantering är generellt sett en grundförutsättning för att kunna hantera informationen på avsett sätt. Brister kan innebära att obehöriga får tillgång till känslig information, att information kan förvanskas av obehöriga, det inte går att följa vem som har gjort vad med informationen och att information man behöver ha tillgång till inte är tillgänglig. Sammantaget skapar informationssäkerhetsbrister risker för förtroendeförluster och i längden obrukbara system. Utveckling inom e-förvaltningsområdet ställer därför höga krav på långsiktigt hållbara och säkra lösningar.

När det gäller informationssäkerhetsarbetet påverkas förutsättningarna för detta i stor utsträckning av tillämplig rättslig reglering. Exempelvis kan ett tydligt utpekat rättsligt ansvar för informationssäkerhetsarbetet göra det enkelt att införa olika nödvändiga säkerhetsåtgärder medan ett otydligt sådant medföra risker att säkerhetsåtgärder inte alls vidtas eftersom ingen ser det som sin uppgift. Informationssäkerhetsperspektivet är särskilt nödvändigt att noggrant analysera och beakta i samband med förslag av den omfattning som nu lagts fram av utredningen och med hänsyn till den information som kommer att hanteras, både avseende mängd och känslighet. En rättslig reglering som stödjer informationssäkerhetsarbetet är av stor vikt.

E-förvaltningsområdet är ett område där det rättsliga regelverket inte alltid utvecklats i samma hastighet som de tekniska möjligheterna vilket innebär risk för rättsliga gråzoner och oklarheter vad gäller uppgifter och ansvar. Stora krav måste ställas på analysen av gällande rätt - särskilt när det gäller tolkning av en grundlag som tryckfrihetsförordningen. Med tanke på de i förlängningen vittgående konsekvenserna av den föreslagna tolkningen behöver analysen även omfatta andra områden än problemområdet för dagen. En tolkning som kan vara effektiv för att lösa ett specifikt och avgränsat problem (allmänna handlingar i eget utrymme) kan framstå som direkt olämplig ur en annan aspekt. I värsta fall kan en ogenomtänkt tolkning innebära att regeln får ett helt annat innehåll än vad lagstiftaren tänkt sig.

Enbart det faktum att man önskar en viss utveckling inom ett område är inte tillräcklig grund för en viss tolkning. Stöd för en rättstolkning bör kunna återfinnas i förarbetena, rättspraxis och den juridiska doktrinen. Utan ett sådant stöd kan man inte med säkerhet fastslå vad som är gällande rätt. Man bör dock kunna utgå från att domstolorna kommer att tolka en grundlag restriktivt – särskilt när det gäller en inskränkning av offentlighetsprincipen – en av våra grundläggande demokratiska principer.

En rättslig analys bör för att vara fullgod omfatta alternativa tolkningar och en kritisk bedömning av analysresultatet. Detsamma gäller analysen av säkerhetsaspekterna vilken måste inkludera riskanalyser. Betänkandet presenterar dock inga alternativa tolkningar och därmed ingen bedömning av alternativa tolkningar. Någon fullvärdig konsekvens- och behovsanalys redovisas inte heller. Det är därför mycket svårt att bedöma förslagen utifrån ett helhetsperspektiv, vare sig man anlägger ett informationssäkerhetsmässigt eller rättsligt perspektiv.

Ett stort ansvar ligger på den som gör den juridiska analysen om analysen ska ligga till grund för utformningen av samhällets e-förvaltning. I värsta fall kan en felaktig tolkning leda till att stora delar av e-förvaltningen måste byggas om utifrån den domstolspraxis som utvecklas på området Detta skulle betyda stora kostnader, stora förtroendebrister och avsevärda olägenheter för såväl medborgaren som myndigheten. Det är därför av stor vikt att bygga på en hållbar grund.

Grunden för E-delegationens förslag: tolkningen av 2 kap 10 § tryckfrihetsförordningen (TF)

E-delegationen definierar *eget utrymme* som ett skyddat förvar hos en myndighet som myndigheten tillhandahåller endast som led i teknisk bearbetning eller teknisk lagring för annans räkning enligt 2 kap. 10 § första stycket TF. Regeln i 2 kap. 10 § första stycket TF är ett undantag från huvudregeln om vad som anses vara förvarat hos en myndighet. Med denna tolkning skulle information som förvaras i det egna utrymmet med andra ord inte anses som allmänna handlingar.

Syftet med att luta sig mot en paragraf som innebär undantag från huvudregeln om allmänna handlingar är huvudsakligen för att säkerställa, i enlighet med E-delegationens tolkning av *användarnas förväntningar*, att informationen som hanteras i detta utrymme:

- inte är tillgänglig för myndigheten som tillhandahåller utrymmet och
- inte kan lämnas ut till andra med stöd av offentlighetsprincipen.

E-delegationen utgår vidare från att dessa förväntningar endast kan uppfyllas genom att de uppgifter som de facto lämnas in till och hanteras av en myndighet i det s k ”egna utrymmet” helt undantas från reglerna om handlingsoffentlighet. Grunden för detta antagande står främst att finna i E-delegationens uppfattning att vissa aktörer känner sig enligt uppgift ”obekväma” med att huvudreglerna om inkomna handlingar tillämpas. Något resonemang om hur denna känsla kan hanteras på annat sätt än att helt sonika undanta uppgifterna från gängse hantering av handlingar hos myndigheter, ex alternativ reglering kopplad med informationsinsatser för att sprida kunskap om regelverket, förs inte. Och detta trots att E-delegationen åtminstone inledningsvis konstaterar att det finns oklarheter kring möjligheten att utvidga tillämpningsområdet för den aktuella undantagsregeln.

E-delegationen konstaterar i den juridiska vägledning (1.0) som togs fram i juli 2013 att *”lagmotiven till undantagsbestämmelserna är skrivna med tanke på annat än IT-baserade tjänster och det finns inte någon rättspraxis som avser t.ex. ärendetjänster. Den för hela e-förvaltningen avgörande frågan om vad som innefattas i endast teknisk bearbetning eller lagring respektive endast befordran av meddelande är därför delvis svår att bedöma.”*

I betänkandet (sid 55) konstaterar däremot delegationen följande: *”I det följande utgår delegationen från att den av sin redovisade tolkning av 2 kap. 10 § första stycket TF är förenlig med gällande rätt. Denna bedömning blir av central betydelse när frågor om sekretess ska bedömas med avseende på information som en myndighet behandlar endast tekniskt.”* Vad som föranleder den förändrade bedömningen framgår inte tillräckligt tydligt.

Visserligen utvecklar delegationen sin syn på tolkningen av 2 kap. 10 § TF i betänkandet men redovisar inget direkt stöd för sin syn i förarbeten, rättspraxis eller ens i juridisk doktrin. Tvärtom synes det saknas stöd i rättskällorna för delegationens tolkning. Uppgiftslämnarutredningen redovisar i sitt betänkande SOU 2013:80 (sid 149 f) en mer nyanserad och resonerande syn på tolkningen av 2 kap. 10 § TF och lyfter, till skillnad från delegationen, även upp potentiella komplikationer med att göra den tolkning som delegationen förordar.

E-delegationens inledande resonemang förefaller förutsätta att delegationens tolkning av 2 kap. 10 § tryckfrihetsförordningen redan är accepterad. MSB är dock inte övertygad om att delegationens tolkning av 2 kap. 10 § TF är gällande rätt utan menar att tolkningen bör utgå från förarbetena till 2 kap. 10 § TF. MSB är fullt medveten om att dagens e-tjänster inte ens fanns i fantasin när

2 kap. 10 § TF utformades men det är frågan om en tolkning av en grundlag och en sådan bör ske restriktivt. Detta förhållningssätt stöds även av existerande rättspraxis. Det ska inte vara möjligt att förändra grundläggande delar av samhällsskicket genom en extensiv tolkning av en grundlag utan den bör ha en stabil och restriktiv tolkning på gott och ont. Att grundlagens regler upplevs hindra utveckling i en viss riktning utgör i sig inte tillräcklig grund för att med hjälp av extensiv och nytänkande tolkning markant utöka tillämpningsområdet hos vissa undantagsregler.

MSB vill återigen betona att en sådan restriktiv tolkning av grundlagen som MSB förordar inte innebär att utvecklingen på e-förvaltningsområdet hindras. De förväntningar som användarna enligt E-delegationen har på hanteringen av information kan uppfyllas med sekretessregler i OSL och ett tillägg i förvaltningslagen – vilket gör att samma mål uppfylls (se MSB:s förslag på alternativ lösning i bilaga 1). Dessutom talar särskilt behovet av rättsligt stöd för informationssäkerhetsarbetet snarare för att denna tolkning skapar bättre förutsättningar för utvecklingen än delegationens förslag. Detta har sin främsta grund i att delegationens lösning skapar ett rättsligt och säkerhetsmässigt vakuum med därpå följande oklara ansvarsförhållanden. Informationen i det egna utrymmet skulle inte vara inkommen till myndigheten men rent fysiskt belasta myndighetens system. Ur ett säkerhetsmässigt perspektiv är det högst tveksamt. Utrymmet skulle i praktiken inte omfattas av någon offentligrättslig reglering. Gallring enligt arkivlagen skulle formellt inte vara möjlig utan utrymmet skulle växa fritt på myndighetens bekostnad. Det går att tolka betänkandet som att det skulle vara straffbart att göra något i utrymmet. För att komma tillrätta med problemet (begränsning av materialet i utrymmet och skadlig eller brottslig data) förutsätts i praktiken ett civilrättsligt avtal mellan medborgaren och myndigheten. Enligt MSB, med stöd i den praxis som finns på området, är det inte godtagbart att förvaltningsrättsliga system regleras genom civilrättsliga avtal mellan medborgaren och myndigheten utan detta bör av rättssäkerhetsskäl ske genom en offentligrättslig reglering.

MSB vill även peka på den diskrepans som råder mellan delegationens förslag att information som finns i det egna utrymmet inte skulle vara inkommen handling och därmed utanför myndighetens rådighet i förhållande till den av Högsta förvaltningsdomstolens fastslagna och betydligt mer utvidgade gränsen för personuppgiftsansvar. I avgörandet HFD 2012 ref. 21, ansågs Försäkringskassan vid tillhandahållande av elektroniska självbetjäningstjänster personuppgiftsansvarig även för behandling som sker innan uppgifterna blir ens tekniskt tillgängliga för kassan. MSB ser ett stort behov av att närmare utreda och analysera förhållandena mellan de båda regelverken. Det väcker en rad frågor kring hur E-delegationens förslag i praktiken ska tillämpas. Hur ska en myndighet kunna ta sitt personuppgiftsansvar i det egna utrymmet? Denna centrala problematik måste utredas närmare.

Sammanfattningsvis anser MSB att delegationens tolkning av 2 kap. 10 § TF inte kan ligga till grund för uppbyggnaden av e-förvaltningen eftersom:

- den troligtvis inte speglar gällande rätt och därför byggs på en mycket osäker grund,
- den skapar osäkerhet i förhållande till personuppgiftsansvarets omfattning, samt att
- den föreslagna lösningen med sina oklara ansvarsförhållanden dessutom begränsar förutsättningarna för att hantera information i det föreslagna systemet med tillräcklig hög säkerhet.

Vägar framåt

Delegationen har föreslagit ett begränsat antal författningsändringar och konstaterar att en helt ny rättslig reglering inte kan införas utan ett omfattande och tidskrävande lagstiftningsarbete och att ett sådant tillvägagångssätt skulle stå i vägen för införandet av moderna e-tjänster under överskådlig tid. Det finns ingen beskrivning av en alternativ reglering, än mindre någon analys, vilket gör att remissinstanserna inte har något sätt att bilda sig en egen uppfattning och ta ställning till detta påstående. Betänkandet ger därför i viss utsträckning intryck av att delegationens förslag är den enda praktiskt möjliga vägen framåt.

MSB själv har, med en trots allt begränsad insats, dock kunnat ta fram ett alternativt rättsligt upplägg som vid diskussioner med sakkunniga på området har setts som en väg värd att analysera vidare i arbetet med att uppnå rättslig stabilitet och förutsebarhet samt ge goda förutsättningar för informationssäkerhetsarbetet såväl som utvecklingen inom e-förvaltningsområdet. Förslaget redovisas i bilaga 1.

MSB har även gjort en genomgång av olika informationssäkerhetaspekter som aktualiseras i samband med utveckling av e-förvaltning och hur dessa behöver hanteras för att uppnå tillräcklig nivå av skydd för informationen som hanteras. Genomgången redovisas i bilaga 2.

Som inledningsvis anfördes så ser MSB positivt på en utveckling av e-förvaltningsområdet givet att denna utveckling vilar på en stabil rättslig grund samt använder sig av lösningar som uppfyller krav på integritetsskydd och informationssäkerhet. Området har en mycket stor betydelse för samhällets funktion och förtroendet för den offentliga sektorn. Dess framtida utveckling, med alla resurser detta kommer att kräva, kan därför inte vila på en oklar rättslig grund och där inte heller säkerhets- och integritetsfrågor beaktas i tillräcklig utsträckning. Det finns fortfarande ett stort behov av fördjupad och brett förankrad analys av olika vägar framåt.

I detta ärende har generaldirektör Helena Lindberg beslutat. Myndighetsjuristen Per-Olof Wikström har varit föredragande. I den slutliga handläggningen har också chefsjuristen Key Hedström, juristen Helena Andersson och enhetschefen Fia Ewald deltagit.

Helena Lindberg

Per-Olof Wikström

Bilaga 1.

MSB:s förslag på rättslig reglering av eget utrymme

Efter att ha analyserat såväl juridiken som säkerhetsfrågorna kopplade till förslaget om ”eget utrymme” och e-tjänsterna har MSB bedömt att E-delegationens förslag behöver justeras för att kunna säkerställa att tjänsterna utformas med tillräckligt hög informationssäkerhet och vila på en stabil juridisk grund. Det är centralt att betona att målbilden med en effektiv e-förvaltning är densamma som delegationens. Det vill säga man når samma mål, med delvis andra medel, vilket resulterar i att e-förvaltningen vilar på en stabilare rättslig grund samt dessutom ges goda förutsättningar att hantera informationssäkerhetsfrågorna.

Utgångspunkterna för MSB:

- Informationshanteringen i det egna utrymmet ska uppfylla relevanta krav på tillgänglighet, riktighet, konfidentialitet och spårbarhet.
- Ansvaret för informationen ska vara tydlig.
- Verksamhetsnära lösningar som ansluter till statliga och kommunala myndigheters ärendehantering ska utnyttjas.
- Rättvisande analogier ska i möjligaste mån användas.
- Den enskildes förväntningar på att användningen av ett eget utrymme infrias ska säkerställas.
- Långsiktig rättslig förutsebarhet ska säkerställas genom att så långt möjligt nyttja huvudreglerna i TF och lagen (2009:400) om offentlighet och sekretess (OSL).

MSB har även beaktat :

- att informationen kan bli föremål för utlämningsbegäran från polisen, och
- att näringslivet kan uppleva ett bristande förtroende till tjänster som nyttjar eget utrymme.

Säkerhetskrav

MSB:s analys visar att hanteringen av information i en ärendetjänst och ett eget utrymme behöver struktureras för att kunna säkerställa att informationen omgärdas av den säkerhet som både användaren och myndigheten/kommunen som erbjuder tjänsten har rätt att kräva. Det handlar främst om att säkerställa[1]

- ett förutbestämt innehåll
- en förutbestämd form

[1] Säkerhetskraven motiveras närmare i bilaga2

- ett tydligt ansvar för hantering av personuppgifter och övrig säkerhet
- en förutbestämd och begränsad tid för hantering av information i eget utrymme, (regler om gallring) och
- en tydlig funktion för användaren att signalera att informationen är färdigställd och kan börja hanteras av myndigheten, exempelvis signering.

För att uppnå detta är det enligt MSB:s mening även av avgörande betydelse att koppla informationshanteringen till myndighetens ärendehanteringsprocess och inte minst rutinerna kring arkivering.

Med hänsyn till behoven av att hitta en lösning som tar hänsyn till inte bara användarnas förväntningar utan även säkerhetsmässiga behov ser MSB det som problematiskt att välja den föreslagna vägen där den information som användaren hanterar i det egna utrymmet inte skulle anses vara allmänna handlingar på grund av undantaget i TF. Anledningarna är flera. Framförallt handlar det om att det finns ett behov av att tydligt kunna reglera vissa centrala säkerhetsaspekter avseende informationshanteringen. Möjligheterna till detta och en tydlig ansvarsfördelning försämras avsevärt om man väljer att luta sig mot undantaget i 2 kap. 10 § första stycket TF. En annan central anledning är som påtalats tidigare att det idag fortfarande råder osäkerhet kring om undantaget i 2 kap. 10 § första stycket TF kan och bör tillämpas på den här typen av situationer. MSB uppfattar den föreslagna användningen av undantaget som en utvidgning av tillämpningsområdet, en utvidgning som potentiellt kan få långtgående konsekvenser för tolkningen av offentlighetsprincipen. Denna osäkerhet i sig skapar även problem för säkerhetsarbetet eftersom grundförutsättningarna för uppbyggnaden av tjänsten inte är tillräckligt utredda och därmed kan komma att förändras i framtiden.

Med en säker informationshantering och användarnas förväntningar i fokus, förordar MSB ett upplägg som utgår från huvudreglerna rörande allmänna handlingar kompletterade med nya regler i offentlighets- och sekretesslagen samt förvaltningslagen. Detta gör det möjligt att säkerställa en tillräckligt hög nivå av informationssäkerhet, skapa förutsebarhet och uppnå E-delegationens målbild. För det fall en myndighet fortfarande skulle bedöma att nackdelarna med att informationen i det egna utrymmet utgör allmänna handlingar överväger fördelarna ser MSB det som lämpligare att med hjälp av krypteringslösningar göra att informationen inte anses som tillgänglig för myndigheten med tekniskt hjälpmedel och därmed inte förvarad hos myndigheten. Detta alternativ hanterar inte de informationssäkerhetsmässiga utmaningarna men går enkelt att förena med grundlagens huvudregler. Förslaget utvecklas nedan under rubriken ”inte allmänna handlingar”.

Det justerade förslaget i korthet

Allmänna handlingar

Det förslag som tagits fram i syfte att nå E-delegationens målbild men med beaktande av informationssäkerhetsaspekterna går i korthet ut på följande.

1. Informationshanteringen i en ärendetjänst kopplas tydligt till myndighetens/kommunens *ärendeprocess*. Detta skapar förutsägbarhet avseende syftet med det egna utrymmet, förenklar för tillhandahållaren av tjänsten att styra vilken typ av information som ska lämnas, hur den ska lämnas och när.

2. För att undvika att ge intryck av att användaren har tillgång till en lagringsyta i en myndighets/kommuns it-system som denne fritt kan använda för alla typer av egen information och som inte någon annan har någon påverkan över bör begreppet eget utrymme justeras. För att nyansera och tydliggöra syftet med ett eget utrymme föreslås istället att man använder begreppet ”*eget förberedelseutrymme*”. Detta ger användaren en bättre förståelse för hur utrymmet är tänkt att användas.

3. Information i ett eget förberedelseutrymme betraktas som *allmänna handlingar* enligt huvudreglerna i TF. Detta skapar

    a. tydlighet att det är myndigheten/kommunen som har ansvar för informationshanteringen och säkerhetsarbetet,

    b. möjlighet att utfärda gallringsföreskrifter för att säkerställa att information som inte längre används gallras från det egna utrymmet på ett rättssäkert och förutsägbart sätt,

    c. trygghet avseende den rättsliga tolkningen och de rättsliga grundförutsättningarna eftersom tillämpningen av undantaget i TF 2:10 idag omgärdas av oklarheter när det gäller elektroniska tjänster.

4. *Ny sekretessreglering* införs vilken säkerställer att en myndighet/kommun är förhindrad att lämna ut information från en användares egna förberedelseutrymme samt säkerställer tystnadsplikt. En möjlig förlaga är den sekretess som råder för växeltelefonister, 40 kap. 4 § OSL.

5. Ny reglering införs i förvaltningslagen och arkivlagen som säkerställer att

    a. det ställs krav på att det egna utrymmet innehåller en *signeringsfunktion* med vilken användaren på ett tydligt sätt kan signalera till myndigheten/kommunen att användaren har färdigställt sitt material och nu lämnar in det till myndigheten/kommunen,

b. handlingen räknas som *inkommen* i förvaltningslagens mening från den tidpunkt då den enskilde signerar dokumenten/formulären,

c. myndigheten/kommunen får inte börja *handlägga ärendet i sak* förrän den signerade handlingen inkommer från användaren. (Motsvarande reglering finns redan i 2 kap. 6 § tullagen (2000:1281)) och

d. användaren arbetar stegvis fram den version som myndigheten ska börja handlägga. I arkivlagen/arkivförordningen tydliggörs att det endast är den version som räknas som inkommen till myndigheten i förvaltningslagens mening som ska arkiveras.

Med detta förslag bedöms E-delegationens och regeringens målbild uppnås. Vidare omhändertas säkerhetsfrågorna, vilket är en förutsättning för att den här typen av tjänster ska kunna åtnjuta förtroende hos både användare och tillhandahållare. I de fall statliga eller kommunala myndigheter redan har utformat tjänster med åberopande av undantaget torde inte funktionen hos/användningen av dessa tjänster påverkas av förslagets genomförande. Snarare kan en tydlig reglering, ex avseende sekretess kopplad till det ”egna förberedelseutrymmet” ge användningen av tjänsterna en långsiktighet eftersom risken för ny praxis på området som försvårar eller utesluter användningen av undantaget undanröjs. Den tydlighet som förslaget ger avseende ansvar både för hanteringen av personuppgifter och skyddet av allmänna handlingar är också central ur ett säkerhets- och användarperspektiv.

Inte allmänna handlingar

För det fall en myndighet gör bedömningen att informationen i användarens egna förberedelseutrymme av olika anledningar inte bör utgöra allmänna handlingar så finns det i huvudsak två alternativa vägar att uppnå detta. I den ena, den som E-delegationen har förordat, väljer myndigheten att betrakta den informationshantering som görs i det egna förberedelseutrymmet som undantagen från reglerna om allmänna handlingar med stöd av 2 kap 10 § TF, d.v.s. myndigheten genomför teknisk bearbetning eller teknisk lagring för annans räkning. Som nämnts ovan är den rättsliga bedömningen av denna lösning osäker. Den innebär även att ansvarsförhållandena rörande informationen blir osäkrare och möjligheterna att gallra faller bort.

Ett alternativ till att uppnå en situation där information i det egna utrymmet inte uppfyller kriterierna på att vara allmänna handlingar är att genom kryptering se till att informationen inte är tillgänglig för myndigheten med tekniskt hjälpmedel. En sådan lösning skulle innebära att informationen (upptagningen) inte uppfyller kraven i 2 kap. 3§ andra stycket TF på att vara förvarad hos myndigheten. Utmaningen är dock att säkerställa att krypteringslösningen ändå inte medger att informationen är tillgänglig, d.v.s.

myndigheten får inte ha tillgång till krypteringsnycklarna. På samma sätt som E-delegationens lösning innebär även krypteringslösningen att ansvarsförhållandena rörande informationen blir osäkrare och möjligheterna att gallra faller bort. Fördelen är dock att den grundar sig på etablerad tolkning av grundlagens regler. Utmaningarna med koppling till informationssäkerhetsaspekterna kvarstår.

Bilaga 2

Närmare om ”eget förberedelseutrymme” och informationssäkerhetsbehov

Precis som E-delegationen har påpekat är informationssäkerhetsfrågorna av betydelse vid verksamhetsutveckling inom e-förvaltningsområdet. Förslaget att underlätta för den enskilde genom att inrätta ett eget förberedelseutrymme ger upphov till flera säkerhetsfrågor eftersom det handlar om att ge en utomstående tillgång till en del av myndighetens/kommunens nät- och it-resurser. I huvudsak aktualiseras säkerhetsfrågorna avseende:

- **Innehåll**: Bristande kontroll över vilken typ av information som läggs in i ett eget förberedelseutrymme och hur länge den ligger där kan orsaka allvarliga säkerhetsproblem. Rätt utformad informationssäkerhet förutsätter kännedom om vilken typ av information man ska skydda och hur länge. I det fall den enskilde har uppfattningen om att denne kan lägga in vilken information som helst och snarast använda det egna utrymmet som en av myndigheten/kommunen fritt tillhandahållen lagringsplats blir det i det närmaste omöjligt att bedöma vilken säkerhetsnivå som krävs. Vidare är det dessutom av avgörande vikt att på en teknisk nivå kunna kontrollera innehållet för att säkerställa att informationen inte innehåller skadlig kod och att den inte kan användas för att begå intrång i övriga delar av systemet. Här krävs därför tydlighet om vilken typ av information som får finnas i det egna utrymmet – det krävs m a o förutsättningar för att skapa ett *förutbestämt innehåll*.

- **Form**: Vilken form som informationen lämnas i har stor påverkan på säkerhetsarbetet. I den utsträckning det är möjligt att styra formen på informationen (exempelvis ett numeriskt värde, en pdf eller liknande) får det en stor och direkt betydelse för säkerhetsarbetet. Förekomsten av skadlig kod kan i hög grad begränsas genom att i det egna utrymmet så långt möjligt endast tillåta informationshantering inom ramen för på förhand framtagna formulär och blanketter. Att begränsa användningen av vissa typer av tecken, att endast tillåta exempelvis numeriska värden, att istället för omfattande möjligheter till fritextskrivande istället begära att få in information på en pdf och på andra liknande sätt påverka formen för informationslämnande skapar avsevärt förbättrade förutsättningar för att skapa säkerhet kring den information som ska hanteras i det egna utrymmet. Användningen av ett eget förberedelseutrymme förutsätter i därför i princip även krav på *förutbestämd form*.

- **Ansvar**: Tydlighet vad gäller vem som är ansvarig för vilken typ av informationshantering är en av de mest avgörande förutsättningarna för ett fungerande säkerhetsarbete. I fallet med eget förberedelseutrymme sker informationshanteringen i en del av myndigheten/kommunens egna it-system. Det är med andra ord i

praktiken endast myndigheten/kommunen som har teknisk och administrativ möjlighet att säkerställa tillräcklig nivå av säkerhet – något som givetvis förutsätter en god kunskap om innehållet, se första punkten. Det är också särskilt uttalat i 31 § personuppgiftslagen att den personuppgiftsansvarige (dvs den som bestämmer ändamål och medlen för behandlingen av personuppgifterna) har ansvar för säkerheten. Lösningar som medför oklarheter om hur långt myndighetens/-kommunens ansvar räcker försvårar arbetet med säkerhet, ett eget förberedelseutrymme förutsätter därför ett på *förhand tydligt uttalat ansvar* för informationssäkerhetsfrågorna.

- **Tidsbestämd hantering**: På samma sätt som oklarheter vad gäller vilken typ av information som finns i det egna utrymmet skapar även oklarheter rörande hur länge informationen finns i det egna utrymmet säkerhetsproblem. Ur ett säkerhetsperspektiv är det av stor vikt att säkerställa att det finns förutsättningar att rensa bort information i det egna utrymmet vid tidpunkter som exempelvis då den enskilde

    - har färdigställt och skickat vidare den information som denne önskar att myndigheten/kommunen hanterar och kvar i det egna utrymmet finns utkast med mera som inte kommer att användas,

    - avlidit eller av annan orsak inte längre kan nyttja det egna utrymmet men fortfarande har information där,

    - på olika sätt missbrukar möjligheterna som användningen av det egna utrymmet erbjuder.

    Bristande möjlighet för den som är ansvarig för säkerhetsarbetet att vid exempelvis ovan nämnda situationer kunna rensa bort information innebär i förlängningen att myndigheten/kommunen behöver säkerställa en möjlighet att under en oviss tid omhänderta en (i värsta fall dessutom okänd) informationsmängd. Ur både ett rättssäkerhetsperspektiv och ett informationssäkerhetsperspektiv är det av stor vikt att det råder *förutsebarhet både avseende att det egna utrymmet kan rensas och vid vilka tidpunkter/under vilka förutsättningar detta sker*.

- **Signeringsfunktion**: Syftet med att ge den enskilde möjlighet att hantera information i det egna utrymmet är att denne ska ges så goda möjligheter som möjligt att förbereda sitt ärende för att sedan ge informationen vidare till myndigheten/kommunen för handläggning. Inte minst för att säkerställa att myndigheten inte i förtid börjar hantera informationen är det av stor vikt att det finns någon typ av signeringsfunktion. Genom att signera informationen elektroniskt signalerar den enskilde att han eller hon är färdig med sin bearbetning och att det nu är myndigheten/kommunen som får fortsätta arbetet. En

elektronisk signering ger även möjlighet att i efterhand kontrollera exakt vilken information som lämnades in för vidare handläggning. Avsaknad av en signeringsfunktion eller motsvarande gör det svårt för både den enskilde och myndigheten/kommunen att bedöma var någonstans hanteringen av informationen befinner sig i ärendehanteringsprocessen. Förfarandet kan i viss utsträckning liknas vid motsvarande upplägg vid e-handel där kunden efter att ha avslutat sina köp markerar detta med att trycka på knappen ”till kassan” eller motsvarande.