Eget utrymme hos myndighet

– en vägledning

eSam

Innehåll

Fakta om eSam

eSamverkansprogrammet (eSam) är en frivillig fortsättning efter E-delegationen och består av 19 medlemmar. Syftet med programmet är att vara ett forum för fortsatt samverkan mellan myndigheter och SKL och ska bygga vidare på de kunskaper och erfarenheter som byggts upp inom ramen för E-delegationen. En viktig uppgift för programmet är att ge ut vägledningar som skapar förutsättningar för att öka den digitala samverkan inom offentlig förvaltning.

Medlemmar är: Arbetsförmedlingen, Bolagsverket, Centrala Studiestödsnämnden, eHälsomyndigheten, Ekonomistyrningsverket, Försäkringskassan, Jordbruksverket, Kronofogdemyndigheten, Lantmäteriet, Migrationsverket, Naturvårdsverket, Pensionsmyndigheten, Polisen, Riksarkivet, Skatteverket, Sveriges Kommuner och Landsting, Tillväxtverket, Transportstyrelsen och Tullverket. (april 2016).

1. Inledning

Eget utrymme har utvecklats till en etablerad myndighetspraxis som fått en omfattande spridning. Exempelvis sjösattes skattedeklaration med eget utrymme redan år 2001. I anknytning till servicetjänster[1] och presentationstjänster[2] tillhandahålls eget utrymme för att användare ska få automatiserad service och kunna hantera sina handlingar utan insyn av utomstående.

Syftet med denna vägledning är att beskriva och förklara de frågor som är centrala när eget utrymme ska utvecklas och användas. Vägledningen ska ses som en vidareutveckling av den beskrivning av eget utrymme och elektroniska tjänster som ges i E-delegationens Juridiska vägledning för verksamhetsutveckling inom e-förvaltningen, version 2.0. eSam ansluter sig till de bedömningar som E-delegationen gjort med de anpassningar som följer av denna vägledning.

Denna vägledning inleds med en allmän beskrivning av eget utrymme och vad som behövs för att utveckla funktioner som är juridiskt korrekta (kap. 2-3). Här behövs samarbete, inte bara mellan verksamhetsutvecklare, säkerhetsspecialister, it-arkitekter, arkivarier och jurister utan även med andra som på något sätt är inblandade i arbetet med att ta fram sådana lösningar (t.ex. beställare, chefer, controllers, kommunikatörer, leverantörer och projektledare m.fl.). Alla dessa yrkeskategorier är därför målgrupp för denna del av vägledningen. Därefter ges en mera juridiskt inriktad genomgång av hur eget utrymme bör utformas och vad som gäller enligt berörda regelverk (kap. 4-5). Slutligen presenteras det behov av olika regler som kan aktualiseras i anknytning till eget utrymme (kap. 6).

Vägledningen redovisar i allt väsentligt endast rättsfrågor som uppkommer när *myndigheter* tillhandahåller eget utrymme åt enskilda.[3]

Arbetet med att ta fram vägledningen har genomförts av eSams rättsliga expertgrupp. Ledamöter i expertgruppen är Johan Bålman, Per Furberg, Sven Granlund, Gustaf Johnssén, Jan Sjösten, Gunnar Svensson, Mikael Westberg, Staffan Wikell, Tomas Öhrn och Christina Wikström. Adjunge-

---

1 Med *servicetjänst* menas, enligt E-delegationens Juridiska vägledning för verksamhetsutveckling inom e-förvaltningen, version 2.0, en e-tjänst där användaren kan (a) utforma utkast till handlingar i ett eget utrymme, (b) i vissa fall få uppgifter förifyllda eller annars utlämnade av den som tillhandahåller det elektroniska utrymmet eller ett annat organ, med stöd av en bastjänst, (c) sända handlingar till ett anvisat mottagningsställe, och (d) vidta andra nödvändiga åtgärder.

2 En *presentationstjänst* är, enligt nämnda vägledning, en e-tjänst där användare får allmänna handlingar visade utan att det som visas ska bli tillgängligt för andra.

3 En utveckling pågår visserligen mot att företag tillhandahåller liknande utrymmen åt enskilda och att handlingar kan ges in till en myndighet med likartat stöd men där aktualiseras endast i begränsade delar motsvarande rättsliga bedömningar som i denna vägledning.

rade ledamöter i expertgruppen är Maria Sertcanli och Nils Fjelkegård. I arbetet har även eSams rättsliga referensgrupp deltagit.

2. Eget utrymme

2.1 Bakgrund

Regeringens mål för it-politiken är att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter. En nödvändig del i denna utveckling är att myndigheter inför fler och mer användbara elektroniska tjänster. Användarna ska både ha nytta av dessa tjänster och få tillräckligt skydd mot manipulationer och missbruk vid användningen av dem.

Eget utrymme tillhandahålls som en service åt användaren. Ingen annan ska få insyn i det material som användare har där. Utrymmet ska samtidigt underlätta för användaren att upprätta och ge in korrekta och fullständiga ansökningar, deklarationer och andra handlingar, men det förekommer också utrymmen som ger stöd åt användare utan att något skickas in till den som tillhandahåller utrymmet. Utkast och liknande handlingar förblir användarens egna handlingar och blir inte att anse som allmänna enligt tryckfrihetsförordningen eller inkomna enligt förvaltningslagen så länge de finns i utrymmet och kriterierna för sådant utrymme är uppfyllda. Uppgifter som finns där ska inte heller annars riskera att röjas genom åtgärder av myndigheten eller myndighetens personal. – Genom egna utrymmen skapas således en allmän tillit till elektroniska tjänster samtidigt som de erbjuder en tillräcklig säkerhet för användaren och förenklar dennes vardag.

I E-delegationens Juridiska vägledning för verksamhetsutveckling inom e-förvaltningen, version 2.0, beskrivs de funktioner som kan finnas i ett eget utrymme för att

- upprätta handlingar,
- skriva under och sända handlingar elektroniskt till myndighetens elektroniska mottagningsställe, och
- motta och förvara handlingar från myndigheter genom
    - en förmedlingstjänst som Min myndighetspost, eller
    - ett personligt hälsokonto eller någon liknande tjänst.

När sådana funktioner används hanteras handlingarna inte i användarens dator, utan i ett elektroniskt utrymme som myndigheten tillhandahåller som en tjänst åt den enskilde.[4] Myndigheten anlitar ofta underleverantörer för it-

[4] E-delegationen har i betänkandet Så enkelt som möjligt för så många som möjligt – Bättre juridiska förutsättningar för samverkan och service (SOU 2014:39) lagt fram förslag till ändringar i lag med avseende på sådana utrymmen. Där används uttrycket elektroniskt förvar i stället för eget utrymme. Syfte är att knyta an till bestämmelsen i 4 kap. 9 § brottsbalken om intrång i förvar. Innebörden avses vara densamma. Eftersom ”eget utrymme” blivit inarbetat i praktiska sammanhang använder vi det här.

drift, överföring via nät och annan teknisk hantering. Det är därför många aktörer inblandade när ett eget utrymme ska tillhandahållas.

Detta sätt att hantera handlingar som finns i eget utrymme inverkar på integritetsskyddet. En myndighet ska inte, genom att tillhandahålla en sådan tjänst, ha insyn i de handlingar som finns där. Detta stöd får inte heller användas på annat sätt så att enskildas personliga förhållanden övervakas eller kartläggs. Därför har E-delegationen och eSam utvecklat en modell för eget utrymme som ger skydd enligt 2 kap. 6 § regeringsformen för enskildas personliga integritet och samtidigt avses tillgodose behov av bl.a. rättssäkerhet och informationssäkerhet; jfr artikel 8 den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) som sedan 1995 gäller som svensk lag.

2.2 Utrymmets utformning

Ett eget utrymme kan beskrivas som en insynsskyddad elektronisk ”plats” där bara användaren får gå in. Utkast till handlingar och annan information ges där en viss juridisk status (se avsnitt 4.1) samtidigt som användaren får service genom att uppgifter automatiserat summeras, förifylls etc.

Det finns olika slag av eget utrymme och de kan förekomma under olika beteckningar. Bland annat används uttrycket ”Mina sidor” ibland med avseende på eget utrymme. I grundutförande finns utrymmet bara under en kort stund, *en viss session,* som vanligtvis avslutas med att en handling som skapats där kan skrivas ut eller ges in till myndigheten eller att det som behandlats i utrymmet tas bort efter att användaren lämnat den webbsida där utrymmet visades. I andra utrymmen kan användaren även mellanlagra sina utkast – i vissa fall också andra handlingar. Då kan användaren hämta sitt material och fortsätta arbetet vid en senare tidpunkt. Ett sådant utrymme kallas *konto.* Är kontot till för säker post kallas det *e-brevlåda;* jfr 5 § förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte.

Användaren ska kunna bruka eget utrymme exklusivt, så att handlingarna i utrymmet skyddas som om de i stället hade hanterats i t.ex. användarens egen datormiljö. Den som tillhandahåller utrymmet behöver således förse detta med ett tekniskt och administrativt skydd för de handlingar som finns där.

Användaren ska kunna utgå från att informationen är skyddad både från offentlighets- och sekretessynpunkt och från persondataskydds- och informationssäkerhetssynpunkt. Den information användaren ser i utrymmet eller annars använder där – den s.k. nyttoinformationen – finns visserligen i myndighetens it-miljö men den ska vara *avgränsad,* i vart fall logiskt, från myndighetens verksamhetssystem. Dessa gränser upprätthålls genom behörighetskontrollsystem, intrångsdetektering och brandväggar m.m. Myndigheten är ansvarig för att informationen i det egna utrymmet från säkerhetssynpunkt hanteras med tillräcklig nivå av konfidentialitet, riktighet och tillgänglighet, samt spårbarhet där så behövs.

2.3 Användargränssnitt och innehåll

Användargränssnittet för användares eget utrymme ska tydligt visa vad som finns där, när en handling sänds därifrån och vilka exemplar som finns kvar där. Utrymmet behöver också utformas så att användaren tydligt uppfattar de uppgifter som finns där som sina privata. Innehar ett företag utrymmet ska företaget på ett självklart sätt kunna se uppgifterna som företagets interna.

Användargränssnittet får alltså inte utformas så att användaren felaktigt får uppfattningen att handlingarna i utrymmet tillhör myndigheten. För att dessa gränser ska bli tydliga behöver utrymmet vara utformat så att inget sänds till en myndighet förrän användaren av utrymmet har klickat på en knapp eller vidtagit någon annan liknande aktiv åtgärd för att sända in handlingen.

Denna gräns mellan en enskilds eget utrymme och myndighetens it-miljö måste vara tydlig även för myndighetens personal. Handläggare och annan personal ska inte få och inte heller kunna bereda sig tillgång till uppgifter i en användares eget utrymme. Detsamma gäller för teknisk personal, med undantag för enstaka personer med särskilt hög behörighet, som behöver vidta åtgärder som är nödvändiga från bl.a. informationssäkerhetssynpunkt. Det kan inte uteslutas att en sådan befattningshavare i något enstaka undantagsfall skulle kunna råka se något i ett eget utrymme, men arbetsuppgiften är inte inriktad på detta informationsinnehåll utan är av rent teknisk eller säkerhetsmässig art.

I syfte att säkerställa en tillräckligt hög nivå av informationssäkerhet behöver myndigheten ställa krav på innehåll och form hos informationen i det egna utrymmet. Det görs bland annat för att minimera risken för att system drabbas av skadlig kod. Det ska även vara tydligt för användaren vilken typ av information det egna utrymmet får innehålla. Det ska inte heller vara tillåtet att förvara information med brottsligt innehåll eller bedriva annan olämplig eller olaglig verksamhet i det utrymme som myndigheten tillhandahåller.

Eget utrymme behöver dessutom utformas så att uppgifter inte bevaras längre än nödvändigt med hänsyn till ändamålet med utrymmet eller att användare brukar sitt utrymme för felaktiga, olagliga eller annars olämpliga behandlingar av personuppgifter.

Det är inte möjligt att generellt, för alla tillämpningar, ange vari kraven på innehåll och form närmare bör bestå. Olika kontroller motverkar att uppgifter röjs[5] för obehöriga, men de erbjuder sällan en sådan säkerhet att kontrollerna aldrig kan kringgås eller annars fallera. Det är många gånger också svårt att verifiera kontrollernas effektivitet och att skapa transparens i denna

[5] Vad som menas med ”röjande” och vilka åtgärder som är möjliga och lämpliga att vidta från juridiska utgångspunkter har redovisats i eSams vägledning Outsourcing – en vägledning om sekretess och persondataskydd.

del, så att det står helt klart att någon otillbörlig hantering av de uppgifter som förvaras i egna utrymmen aldrig kan förekomma.

I ett eget utrymme får det endast finnas stödfunktioner som *användaren* brukar. Detta stöd kan bl.a. bestå i att göra det enklare att fylla i handlingar, summera angivna belopp och få information om vad som bör skrivas i ett visst fält. Till denna service hör också att göra det enkelt för användaren att skriva under eller att på annat sätt avsluta arbetet med ett utkast, så att det inte råder någon tvekan om när handlingen är färdig, vem den härrör från och att angiven utställare står för handlingens innehåll. Det kan dessutom finnas funktioner för att sända iväg handlingar från eget utrymme till ett anvisat mottagningsställe, med hjälp av automatiserad adressering och funktioner för elektronisk överföring till mottagningsstället.

Den personal som sköter eget utrymme får alltså inte ha någon arbetsuppgift som är inriktad på informationsinnehållet i utrymmet; jfr avsnitt 2.5. Manuell service av myndighetspersonal bör endast få förekomma i utrymmet då detta är nödvändigt för att hantera en säkerhetsincident.

2.4 Egen hämtning och egen visning

I ett eget utrymme kan också andra funktioner finnas. Exempelvis kan användare i vissa egna utrymmen hämta handlingar (s.k. egen hämtning) från en annan myndighet eller ett privaträttsligt subjekt.[6] Handlingar som användaren hämtar på det sättet får inte läsas eller annars användas av myndigheten när de finns *i* utrymmet eller under transport dit. Om utrymmet genom sådan egen hämtning ger användaren möjlighet att ta del av innehållet i handlingar som redan finns i myndighetens förvar, t.ex. tidigare inskickade ansökningar eller myndighetsbeslut, skapas det i det egna utrymmet kopior av dessa handlingar. Dessa kopior utgör *andra exemplar* av myndighetens handlingar och tillhör användaren, på samma sätt som om användaren hade sparat kopior i sin egen dator eller på papper hos sig. Där så krävs ur ett informationssäkerhetsperspektiv får myndigheten sätta begränsningar rörande format och innehåll i handlingar som förs in i det egna utrymmet.

I vissa utrymmen finns dessutom funktioner för att användaren ska kunna göra en automatiserad sammanställning och presentation av uppgifter som finns i handlingar där (s.k. egen visning).[7] Användaren kan därmed i sitt utrymme, när en sådan funktion byggts in, få en sammanställning av in-

---

6 Se E-delegationens Juridiska vägledning för verksamhetsutveckling inom e-förvaltningen, version 2.0, avsnitt 4.1.3, 5.2 och 5.4, där egen *hämtning* beskrivs så att uppgift eller handling, med stöd av en bastjänst lämnas ut till en användares eget utrymme, som tillhandahålls åt användaren av ett annat organ än det som lämnar ut uppgiften eller handlingen.

7 Se E-delegationens Juridiska vägledning för verksamhetsutveckling inom e-förvaltningen, version 2.0, avsnitt 4.1.3, 5.2 och 5.4, där egen *visning* beskrivs som en funktion i en e-tjänst, genom vilken uppgifter eller handlingar hämtas in från en eller flera andra myndigheter eller andra organ med stöd av bastjänster, så att materialet automatiserat kan sammanställas och läsas av den enskilde i ett serviceskede i dennes eget utrymme.

formation som finns där utan att myndigheten ser eller annars får ta del av eller använda den. Även här krävs en tydlig gräns mot myndighetens ärendehandläggning.

2.5 Hjälptjänster

Hjälptjänst (s.k. helpdesk) beskrivs i E-delegationens Juridiska vägledning för verksamhetsutveckling inom e-förvaltningen, version 2.0, som en tjänst för att ge hjälp till en användare eller att förklara uppgifter som lämnats till användaren. Information som inkommer till myndigheten i samband med att sådan hjälp ges blir allmän handling hos myndigheten. Det finns *dels* sådana hjälptjänster som är till för att användare ska kunna övervinna tekniska fel eller fel vid användning av tjänsten, *dels* hjälptjänster där kompletterande information ska kunna lämnas muntligen eller skriftligen, om viss information saknas eller användaren inte förstår uppgifter som lämnats elektroniskt.

En hjälptjänst får inte utformas så att handlingar oavsiktligt blir allmänna utan att omfattas av det skydd som användaren har anledning att förvänta sig. En myndighet som planerar en hjälptjänst måste därför vidta särskilda åtgärder för att ge den enskilde det skydd mot insyn i uppgifter vilka finns i utrymmet som han eller hon förväntar sig, se vidare avsnitt 5.3.

Hjälpen ska alltså när det är möjligt lämnas utan att myndighetens verksamhetssystem eller personal får tillgång till information i eget utrymme. I så fall är det tillräckligt att den som ger hjälp inte röjer eller utnyttjar vad han eller hon har fått veta. Det finns emellertid också undantagssituationer där personal i en s.k. hjälptjänst behöver se innehåll i utrymmet för att kunna ge hjälp på ett ändamålsenligt sätt. Särskilda åtgärder måste då vidtas för att handlingar inte ska kunna begäras ut av var och en. Dessa förutsättningar och alternativa vägar att få tillgång till den information som behövs har redovisats närmare i ett betänkande av E-delegationen (SOU 2014:39 s. 93 ff.).[8]

[8] Hjälptjänsterna har där grovt delats in i sådana där den hjälpsökande bara kan läsa information, t.ex. s.k. FAQ, sådana där helt automatiserad hjälp ges respektive tjänster där hjälp ges muntligen vid samtal, med eller utan att uppgifter tillgängliggörs elektroniskt för den som ger hjälpen.

3. Skydd för utrymmet

3.1 Rättsligt skydd

Eget utrymme ska utformas för att ta tillvara det skydd för användaren som reglerna i tryckfrihetsförordningen och offentlighets- och sekretesslagen kan erbjuda. Det ska också införas tydliga regler för hanteringen av utrymmet så att nyttoinformationen i utrymmet skyddas.

Eget utrymme ska utformas så att endast användaren förfogar över handlingar i utrymmet och så att dessa handlingar inte blir att anse som

- allmänna enligt tryckfrihetsförordningen, i det följande ”TF”, eller
- inkomna enligt förvaltningslagen (1986:223), i det följande ”FL”.

Detta hindrar inte att ett exemplar av en handling i utrymmet kan ha sänts till en myndighet och blivit allmän handling där, samtidigt som ett annat exemplar av handlingen finns kvar i utrymmet; jfr hur olika regler gäller enligt 2 kap. 10 § andra stycket TF för material i elektroniska akter som finns i en myndighets verksamhetssystem (är allmänna handlingar) respektive säkerhetskopior av detta system (är inte allmänna handlingar), se vidare avsnitt 5.1.1.

Uppgifterna i det egna utrymmet ska också vara skyddade av sekretess enligt offentlighets- och sekretesslagen (2009:400), i det följande ”OSL”, och av bestämmelser om straff för intrång i enskildas informationstillgångar.

För eget utrymme behövs därför tydligt utformade instruktioner, avtalsvillkor eller föreskrifter som förbjuder myndighetens personal och andra att bereda sig tillträde till annans utrymme eller att på annat sätt ta del av eller missbruka information i utrymmet, med undantag för när detta blir nödvändigt för att tillgodose behovet av informationssäkerhet. Dessa regler ska anpassas till de arbetsrättsliga, avtalsrättsliga, straffrättsliga och straffprocessuella sanktionsmekanismer som redan finns, så att dessa skyddar användares eget utrymme. Exempelvis bör en myndighet som tillhandahåller ett utrymme, vid misstanke om att ett brott har begåtts i eller genom ett eget utrymme, inte ge brottsutredande organ tillgång till information i utrymmet utan att användaren har lämnat sitt samtycke eller att polis eller åklagare har beslutat om ett straffprocessuellt tvångsmedel som t.ex. husrannsakan.

3.2 Informationssäkerhet

Olika samverkande åtgärder behöver vidtas för att ge eget utrymme ett tillräckligt skydd mot obehörig åtkomst och annat missbruk.

Det räcker inte att användaren ser sig vara i eget utrymme och att lämpligt utformade regler ger de handlingar som finns där beskrivet juridiskt skydd. Det krävs också tillräckliga säkerhetsarrangemang. Myndigheten som tillhandahåller det egna utrymmet är ansvarig för att upprätthålla en tillräcklig nivå av säkerhet. Av 31 § personuppgiftslagen (1998:204), i det följande

”PuL”, följer att den personuppgiftsansvarige är skyldig att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas i utrymmet. Uppgifter som förvaras i eget utrymme kan därför behöva skyddas genom olika former av persondataskyddande teknik, för att vissa risker för intrång i den personliga integriteten aldrig ska kunna uppstå.

Även andra regleringar ställer krav på att informationen hanteras på ett tillräckligt säkert sätt. I 19 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap föreskrivs om varje myndighets ansvar för säker informationshantering. Ansvaret gäller även när myndighetens information hanteras av en extern aktör eller när myndigheten tillhandahåller andra aktörer tjänster för informationshantering inom e-förvaltning eller motsvarande. Myndigheten för samhällsskydd och beredskap har utfärdat föreskrifter som förtydligar hur statliga myndigheter ska arbeta med informationssäkerhet. Enligt föreskrifterna (MSBFS 2016:1) är myndigheten skyldig att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet.

Ett ledningssystem för informationssäkerhet är ett sätt för organisationens ledning att på ett systematiskt sätt styra arbetet med informationssäkerhet i syfte att planera, genomföra, kontrollera, följa upp, utvärdera och förbättra säkerheten i verksamhetens informationshantering. Skyddet för det egna utrymmet utgör en del i detta arbete.[9] I syfte att säkerställa ett adekvat skydd för uppgifterna i det egna utrymmet och att kunna hantera hot och risker behöver myndigheten som ett första steg klassificera den information som det egna utrymmet ska innehålla med utgångspunkt i konfidentialitet, riktighet och tillgänglighet i olika nivåer utifrån vilka konsekvenserna som kan uppstå av ett bristande skydd. Klassificeringen ska även omfatta spårbarhet där så behövs. Därefter behöver hot och risker för det egna utrymmets information, system och tjänster identifieras och analyseras. En sådan riskanalys för eget utrymme behöver innefatta hela den kedja av behandlingar som kan bli aktuella.

Utifrån informationsklassificeringens resultat och den genomförda riskanalysen identifieras och vidtas därefter de tekniska och organisatoriska åtgärder som krävs för att uppfylla skyddsbehovet. Exempelvis behöver tekniska metoder för tillträdesbegränsning och behörighetskontroll införas. Krypteringsmekanismer för att ge skydd mot obehörig insyn och förändring kan också behövas. Det systematiska informationssäkerhetsarbetet innebär även att vidtagna åtgärder och gjorda bedömningar följs upp och utvärderas. Detta görs för att kontinuerligt utveckla skyddet för att över tid upprätthålla informationens och det egna utrymmets behov av säkerhet.

Säkerhetsåtgärder som kopplas till det egna utrymmet behöver även utformas så att myndigheten kan uppfylla de krav på obligatorisk it-incidentrapportering som följer av 20 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. Myndig-

[9] Stöd för systematiskt informationssäkerhetsarbete finns samlat på www.informationssäkerhet.se.

heten för samhällsskydd och beredskap har utfärdat närmare föreskrifter om verkställigheten av kravet på it-incidentrapportering.[10]

[10] Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters rapportering av it-incidenter (MSBFS 2016:2).

4. Juridisk utformning

4.1 Utrymmets juridiska status

Eget utrymme ska anpassas till gällande rätt genom att konstrueras så att det uppfyller rekvisiten i vissa rättsregler.

Eget utrymme ska vara utformat så att

- handlingar i utrymmet
  - behandlas endast som led i teknisk bearbetning eller teknisk lagring för annans räkning (2 kap. 10 § första stycket TF),
  - inte anses ha anlänt till myndigheten eller kommit en behörig tjänsteman till handa (10 § FL),
- reglerna om persondataskydd inte måste tillämpas så att den myndighet som tillhandahåller utrymmet behöver ta del av information i utrymmet,
- normalt ingen annan än användaren av utrymmet får bereda sig tillgång till det användaren har i utrymmet eller annars förfoga över dennes information; jfr exempelvis 4 kap. 9 a – 9 c §§, 10 kap. 5 § och 20 kap. 3 § brottsbalken,[11]
- en handling som avses vara privat omedelbart får gallras om den råkat hanteras så att den blivit allmän (arkivförfattningar), och
- information som behandlas i utrymmet eller i anknytning till utrymmet endast för att upprätthålla en fungerande, effektiv och säker drift av eget utrymme är sekretessreglerad i den omfattning som krävs; jfr avsnitt 5.3.

I denna vägledning redovisas hur dessa juridiska förutsättningar uppnås inom ramen för gällande rätt. Redovisningen utgår från tolkningar som myndigheter har tillämpat sedan länge. I det enskilda fallet blir det emellertid fråga om en bedömning av gällande rätt som varje myndighet måste göra själv och som i många delar inte har prövats i rättspraxis. Denna vägledning beskriver därför också

- rättsliga risker,
- vad som särskilt bör beaktas för att minimera risker, och
- hur myndigheter kan förfara om en risk förverkligas.

[11] Jfr dock vad som beskrivs om teknisk personals åtgärder för att exempelvis upprätthålla en tillräcklig säkerhetsnivå eller hantera en incident.

4.2 Utrymmets egenskaper och användarens förväntningar

Myndigheten ska utforma eget utrymme så att endast användaren tar del av uppgifter i eget utrymme och att utrymmet inte missbrukas.

Myndigheten ska ha utrett

- att tillhandahållandet av eget utrymme ryms inom myndighetens uppgifter, som följer av myndighetens instruktion, andra författningar, regleringsbrev eller andra särskilda beslut,[12]
- vilken information som är tänkt att hanteras i det egna utrymmet och vilka krav den ställer på konfidentialitet, riktighet och tillgänglighet samt spårbarhet där så behövs,
- hur utrymmet ska regleras – genom föreskrifter eller avtal – och utformas praktiskt för att de handlingar som finns där ska förbli användarens privata när de är i utrymmet,
- vilka risker som finns för missbruk av utrymmet, hur en risk ska motverkas och hur myndigheten ska uppfylla sitt ansvar för dess it-miljö och skyddet av användarens eget utrymme, och
- hur persondataskyddet ska hanteras för att den myndighet som tillhandahåller utrymmet inte ska behöva ta del av information i en användares eget utrymme.

En viktig del i detta arbete är att införa tekniska, administrativa och juridiska begränsningar så att eget utrymme inte kan, eller i vart fall inte får, användas av den enskilde för annat än vad tillhandahållaren avsett. Som exempel kan nämnas att tydliga instruktioner behöver ges till användaren om vad utrymmet avses användas till och att fritextfält bör begränsas så långt möjligt, t.ex. med användningen av formulär med fasta svarsalternativ. Vidare bör rimlighetskontroller och liknande införas inte bara för att minimera fel utan även för att förhindra eller i vart fall motverka otillåten användning. Dessutom behöver processer finnas på plats som säkerställer att tekniska kontroller av innehållet genomförs i syfte att upptäcka skadlig kod och otillåten information.

Användaren ska kunna utgå från att utrymmets innehåll är privat, att myndigheten skyddar det mot obehörig åtkomst eller användning, tryggar dess riktighet och tillgänglighet samt att de *exemplar* av handlingar som finns i utrymmet *inte*

- anses vara

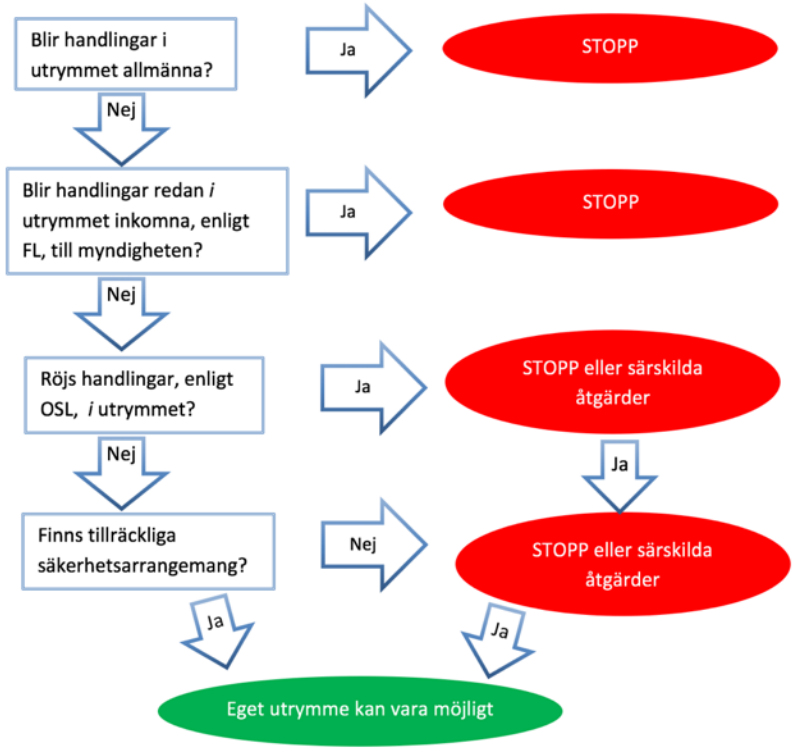
---

[12] Det finns en skiljelinje mellan *privaträttsliga subjekts* principiella rätt till ett fritt agerande och *myndigheters* åligganden att *fullgöra bestämda uppgifter* i det allmännas tjänst. En myndighet ska i princip ha stöd i lag eller annan författning för sina åtgärder (legalitetsprincipen), se kap. 5.6. För kommuner och landsting gäller dessutom den allmänna kommunala kompetensen enligt 14 kap. 2 § RF samt 2 kap. 1 § kommunallagen (1991:100).

– allmänna och offentliga handlingar, eller
– inkomna till myndighet enligt förvaltningslagen,

- granskas av den tjänstelevererande myndighetens personal för att t.ex. informera den registrerade, rätta felaktiga uppgifter i en handling i utrymmet, ta bort aktivt material eller vidta annan åtgärd i egenskap av tillhandahållare av utrymme, eller
- röjs muntligen eller i skrift eller annars används av den tjänstelevererande myndigheten eller dess personal.

Det behöver därför också finnas regler och funktioner för att rensa bort uppgifter som inte längre behövs i ett eget utrymme; se även följande figur över de huvudfrågor som tillhandahållare av eget utrymme behöver överväga.



4.3 Automatiserad service

Service kan erbjudas helt automatiserat i användares eget utrymme, utan att handlingar i utrymmet anses vara inkomna till myndigheten.

Till eget utrymme hör automatiserade funktioner som delvis styr hur utrymmet används. Som exempel kan nämnas utrymmen där uppgifter förifylls, där rimlighetskontroller och sammanräkningar görs av det användaren skriver och där användaruppgifter stäms av mot offentliga register. I utrymmet får bara sådana stödfunktioner finnas som myndigheten tillhandahåller helt automatiserat. Myndigheten ska inte få ta del av innehållet i utrymmet.

Så länge användaren inte sänt en handling från utrymmet har den inte kommit in enligt förvaltningslagen (se avsnitt 5.2). Detta gäller oberoende av vilka automatiserade funktioner som erbjuds i eget utrymme, eftersom det ska ha reglerats så att myndigheten inte får ta del av de handlingar som finns

där. Något förvaltningsärende har under sådana förhållanden inte anhängiggjorts. Handlingen finns endast i utrymmet; se vidare avsnitt 5.2.2 om tekniska hinder mot att ge in en handling.

Eftersom utrymmet tillhandahålls endast för teknisk lagring och teknisk bearbetning för utrymmesinnehavarens räkning – alternativt att driften av utrymmet utkontrakterats så att handlingarna inte är tekniskt tillgängliga för myndigheten – anses de inte heller vara allmänna enligt tryckfrihetsförordningen (se avsnitt 5.1).

Kortfattad checklista

- Ryms tillhandahållande av eget utrymme inom myndighetens uppdrag eller, vad gäller kommuner och landsting, befogenheter i övrigt?
- Behandlas uppgifter i utrymmet bara för användarens räkning?
- Finns det risk för att myndighetens personal får del av uppgifter i användares utrymme eller att en handling i utrymmet hamnar i myndighetens verksamhetssystem utan användarens vilja och avsikt?
- Är användarens hantering av uppgifter i utrymmet reglerad och ansvarsfördelningen mellan användaren och myndigheten tydlig?
- Har myndigheten klassificerat den information som är tänkt att finnas i det egna utrymmet utifrån dess behov av konfidentialitet, riktighet och tillgänglighet, samt spårbarhet där så behövs?
- Finns det risk för att användaren missbrukar sitt utrymme eller att utrymmet inte är tillräckligt skyddat mot missbruk av annan?
- Kan regler om persondataskydd eller om informationssäkerhet föra med sig att myndigheten måste ta del av innehåll i eget utrymme?
- Har myndigheten övervägt vilka rättsliga risker som följer med att tillhandahålla utrymmet och den service som ges där samt hur myndigheten kan förfara om en risk förverkligas?

5. Berörda regelverk

Myndigheter tillhandahåller elektroniska tjänster av varierande slag och egna utrymmen med delvis olika funktioner. Många rättsområden kan därför bli berörda. Här redovisas regelverk av generell betydelse för eget utrymme.

5.1 Handlingsoffentlighet

En användares eget utrymme ska utformas så att bara användaren får ta del av de uppgifter som finns där. Därför får uppgifter i eget utrymme inte bli allmänna handlingar.

5.1.1 En myndighet tillhandahåller eget utrymme

Tillhandahåller en myndighet eget utrymme under sådana former att myndigheten får tillgång till användarens information *endast* som led i teknisk bearbetning eller teknisk lagring för användarens räkning blir de handlingar som finns där inte allmänna. Skulle en myndighet för sin egen räkning använda information som finns i det tillhandahållna utrymmet är utrymmet emellertid inte användarens ”eget”. Det behövs därför en tydlig gräns mellan handlingar som bara hanteras av användaren själv i det egna utrymmet och handlingar som användaren har sänt till myndigheten från utrymmet.

Enligt 2 kap. 3 § första stycket TF är en *handling*[13] allmän om den *förvaras* hos myndighet och enligt 2 kap. 6 eller 7 §§ är att anse som *inkommen* till eller *upprättad* hos myndighet. För elektroniska handlingar i ett eget utrymme gäller enligt 2 kap. 3 § andra stycket TF att de är *förvarade* hos myndighet om de är *tillgängliga* för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i uppfattbar form.[14]

Information som en användare har i eget utrymme skulle alltså, om endast nämnda regler beaktas, bli allmän handling om utrymmet tillhandahålls av

---

[13] Legaldefinitionen i 3 § av handling är utformad så att det knappast kan råda någon tvekan om att data i eget utrymme innefattas. ”Med handling förstås framställning i skrift eller bild samt upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel.”

[14] Detta förvaringsrekvisit för elektronisk miljö har samordnats med en regel i 2 kap. 6 § första stycket TF om när en elektronisk handling anses vara inkommen. Så anses vara fallet när *annan* har *gjort den tillgänglig* för myndigheten på sätt som anges i 3 § andra stycket; dvs. med *tekniskt hjälpmedel* som myndigheten *själv utnyttjar* för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas. Cirkeln är därmed sluten. Är handlingen förvarad är den också inkommen, om ”annan har gjort den tillgänglig” på angivet sätt. Regeringen har förklarat att det räcker att en person hos myndigheten, t.ex. på teknikavdelningen, har tekniska möjligheter att överföra uppgifter i uppfattbar form för att sammanställningar av dessa uppgifter ska utgöra allmänna handlingar (prop. 2007/08:160 s. 71).

myndighet och innehållet inte krypteras eller på annat sätt görs tekniskt otillgängligt för myndigheten (se dock även avsnitt 5.1.2). Av 2 kap. 10 § första stycket TF följer emellertid att en handling som förvaras hos en myndighet *endast* som led i teknisk bearbetning eller teknisk lagring för annans räkning inte anses som allmän handling hos den myndigheten.[15]

Eget utrymme ska vara utformat så att detta undantag blir tillämpligt på användarens information i utrymmet. Myndigheter som tillhandahåller eget utrymme måste dock se upp så att utrymmet inte får en felaktig utformning. Utför tillhandahållaren, eller driftsleverantören, andra åtgärder än teknisk bearbetning eller lagring är undantaget inte längre tillämpligt.[16] I så fall kan utrymmesinnehavarens handlingar bli allmänna och sakna skydd från insyn om uppgifterna i dem inte omfattas av sekretess.

Som exempel på teknisk *bearbetning* anges i de något ålderstigna förarbetena bl.a. tryckning, kopiering, redigering av ljudupptagningar och överföring av sådana upptagningar till grammofonskiva (a. prop. s. 171 som hänvisar till s. 137). Som exempel på teknisk *lagring* anges sådana former av lagring som kräver tekniska anordningar, t.ex. lagring av information i skivminne eller på magnetband. Exakt vilka åtgärder som utgör enbart teknisk bearbetning eller teknisk lagring i dagens elektroniska verklighet är i någon mån osäkert. Av praxis framgår att åtgärder som mottagaren utför *för egen räkning* och som innebär en *bearbetning av handlingarnas faktiska innehåll,* t.ex. genom att uppgifter används för framställning av statistik eller arbetsmiljörapporter, inte omfattas av undantaget (jfr HFD 2011 ref. 52).

De åtgärder som avses i denna vägledning, dvs. sådana tjänster som helt utförs elektroniskt och automatiserat för utrymmesinnehavararens räkning, omfattas dock enligt eSams bedömning av undantaget för teknisk bearbetning och teknisk lagring.[17] Detta innebär att ett exemplar av en handling som finns kvar *i* utrymmet kan ha mångfaldigats, så att ett annat exemplar med samma innehåll sänts till en myndighets elektroniska mottagningsställe och blivit allmän handling där. Kammarrätten i Stockholm har också i en dom den 26 oktober 2015 (mål nr. 7369-15) funnit att handlingar i eget ut-

---

15 På motsvarande sätt följer det av 2 kap. 6 § tredje stycket TF att en handling som återkommer till en myndighet efter teknisk bearbetning eller teknisk lagring inte anses som en inkommen handling där. Detta undantag är av relevans om myndigheten anlitar en extern leverantör för drift av tjänsten. Rimligen bör den information som finns i eget utrymme, och som genom utkontrakteringen av it-driften görs tekniskt tillgänglig för denne, inte heller anses expedierad från, och därmed en upprättad allmän handling hos, den avsändande myndigheten. En annan tolkning skulle leda till att undantaget i 2 kap. 6 § tredje stycket TF skulle förlora sin funktion; jfr avsnitt 4.2 eSams vägledning Outsourcing – en vägledning om sekretess och persondataskydd.

16 Det gäller bara när hanteringen sker ”endast” som led i teknisk bearbetning eller teknisk lagring för annans räkning.

17 För ett utförligt resonemang kring undantaget för teknisk bearbetning och teknisk lagring hänvisas till E-delegationens betänkande Så enkelt som möjligt för så många som möjligt, SOU 2014:39 s. 44 ff.

rymme inte är att anse som allmänna och att det därvid ligger i sakens natur att vissa anställda har åtkomst till berörd databas för att administrera den.

5.1.2 Driften av eget utrymme utkontrakteras

Om en myndighet som erbjuder eget utrymme åt användare utkontrakterar driften av tjänsten har myndigheten inte teknisk tillgång enligt 2 kap. 3 § andra stycket TF till de handlingar som finns i dessa utrymmen. Är driftleverantören en myndighet kan det undantag från allmän handling som föreskrivs i 2 kap. 10 § första stycket TF tillämpas.

En myndighet kan i vissa fall låta en extern tjänsteleverantör sköta driften av egna utrymmen som myndigheten tillhandahåller åt användare. Sådan s.k. outsourcing eller utkontraktering är en del i myndigheternas strategier för att utveckla e-förvaltningen. När driften av eget utrymme har utkontrakterats finns de handlingar som användare hanterar i eget utrymme hos driftleverantören, inte hos den myndighet som i juridisk mening tillhandahåller utrymmet åt användaren. Av tekniska lösningar, outsourcingavtal och andra regler som rör ett utrymme kan följa att den myndighet som lagt ut driften inte har tillgång till information som en användare har i ett eget utrymme.[18]

Under sådana förhållanden gäller istället huvudregeln i 2 kap. 3 § andra stycket TF. Enligt den anses en upptagning bli allmän handling när den *är tillgänglig för myndigheten* med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att handlingen kan läsas, avlyssnas eller på annat sätt uppfattas.

Den myndighet som erbjuder eget utrymme bör alltså inte – när driften av utrymmet är utkontrakterad – ha tillgång till de handlingar som finns där. Detta bör återspeglas i de avtal och andra överenskommelser som träffas mellan den myndighet som tillhandahåller eget utrymme åt användaren och driftleverantören. Att myndigheten elektroniskt, via t.ex. e-post, skulle kunna framställa en begäran om att vissa uppgifter ska lämnas ut ur ett eget utrymme innebär inte annat än att driftleverantören ska pröva frågan om och i så fall vilka uppgifter som ska lämnas ut – inte att begärande myndighet har teknisk tillgång till uppgifterna. Myndigheten får därmed, oberoende av om driften av utrymmet är utkontrakterad till en myndighet eller ett privaträttsligt organ, inte sådan tillgång till handlingar som avses i 2 kap. 3 § andra stycket TF.[19]

---

[18] Uppdraget till driftleverantören är alltså inte att upprätta eller annars hantera handlingar som tillhör myndigheten; jfr t.ex. RÅ84 2:49 och JO:s beslut den 23 januari 2014 (dnr. 3529-2012).

[19] Högsta förvaltningsdomstolen har i en dom den 29 oktober 2015 (mål nr. 1356-14) funnit att det inte finns sådan teknisk tillgång som avses i 2 kap. 3 § andra stycket TF när en myndighet inte på egen hand kan söka i en annan myndighets uppgiftssamling, utan får framställa en begäran om att vissa uppgifter ska lämnas ut, och den myndighet som mottar begäran *förfogar över* frågan om och i så fall vilka uppgifter som ska lämnas ut.

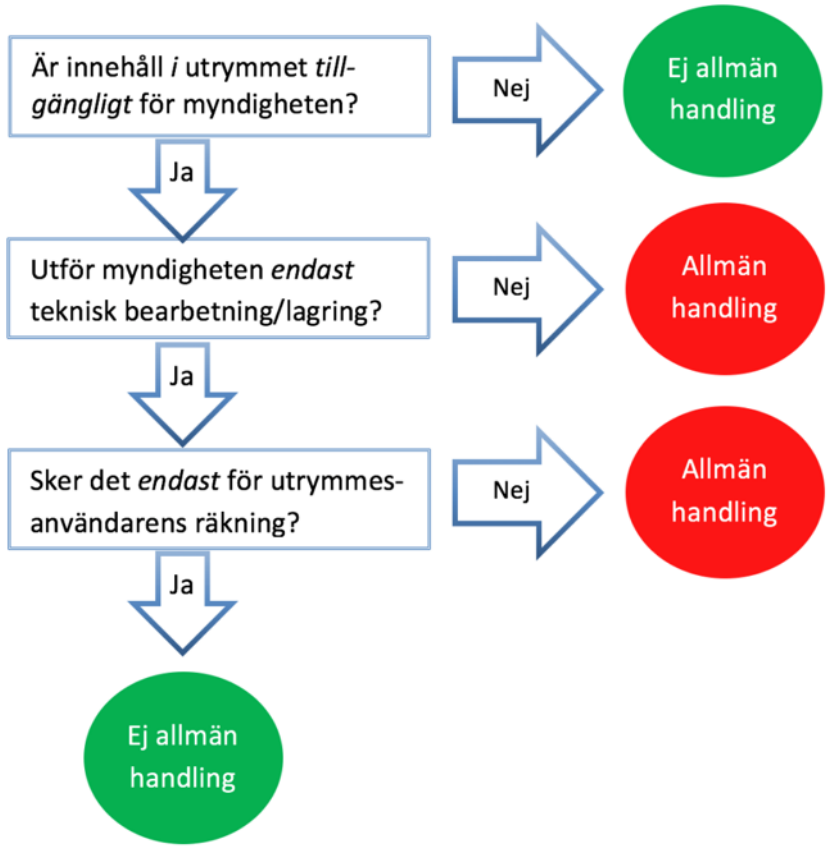
Det kan emellertid inte uteslutas att en *myndighet som tillhandahåller* eget utrymme åt enskilda väljer en sådan utformning av it-driften att inte bara driftleverantören utan även myndigheten får anses förfoga enligt 2 kap. 3 § andra stycket TF över frågan om och i så fall vilka uppgifter som ska lämnas ut. I så fall kan i stället 2 kap. 10 § första stycket TF bli tillämplig i enlighet med vad som har redovisats i avsnitt 5.1.1.

Är *driftleverantören* en myndighet eller ett annat organ hos vilket reglerna om handlingsoffentlighet gäller följer det av 2 kap. 10 § första stycket TF att handlingarna hos underleverantören inte blir att anse som allmänna där. Av outsourcingavtal och andra regler behöver följa att leverantören inte får använda uppgifterna för egen räkning. – Aktörerna måste se upp så att denna begränsning upprätthålls och att dessa krav blir tillgodosedda när berörda funktioner ska utformas, upphandlas, regleras och tas i drift.

Checklista beträffande handlingsoffentlighet

- Kan myndigheten genom kryptering eller annan teknisk lösning utforma eget utrymme så att informationen i utrymmet inte blir tekniskt tillgänglig enligt 2 kap. 3 § TF för någon inom myndigheten, inte ens för tekniker med högsta behörighet i myndighetens it-miljö?
- Kan myndigheten – om ett heltäckande hinder mot teknisk åtkomst för myndighetens personal inte går att införa – begränsa åtkomsten så att informationen bara används för teknisk lagring och teknisk bearbetning för annans, inte för egen, räkning?
- Är personalens hantering av uppgifter i eget utrymme tydligt reglerad?
- Utkontrakteras driften av eget utrymme? Har den tekniska hanteringen och avtalen i så fall utformats så att handlingar i eget utrymme, som finns hos driftleverantören, inte är tillgängliga för den myndighet som erbjuder eget utrymme åt användare?
- Finns det någon plan för hur myndigheten ska agera för att skydda enskilda om hanteringen av eget utrymme skulle fallera så att handlingar oavsiktligt blir allmänna?
- Finns det en tydlig punkt för att sända iväg handling från eget utrymme och tydliga avgränsningar i övrigt så att det inte kan finnas någon tvekan om vad som är användarens material respektive myndighetens material?

Se även följande figur över de huvudfrågor som tillhandahållare av eget utrymme behöver överväga rörande handlingsoffentlighet.



5.2 Förvaltningslagen

5.2.1 Inkommande och service

En handling som sänts till en myndighets elektroniska mottagningsställe anses ha kommit in enligt 10 § FL när den har tagits emot där. Myndigheten bör anvisa ett elektroniskt mottagningsställe dit meddelanden kan sändas, skicka kvittens när ett meddelande nått mottagningsstället och underrätta avsändaren om mottaget meddelande till någon del inte kunnat uppfattas.

Enligt 4 § FL ska varje myndighet lämna upplysningar, vägledning, råd och annan sådan hjälp till enskilda i frågor som rör myndighetens verksamhetsområde. För sådant s.k. faktiskt handlande, t.ex. att tillhandahålla tekniskt och administrativt stöd för att enskilda ska kunna ge in handlingar elektroniskt, gäller FL:s regler om service. Hjälp lämnas i den utsträckning som är lämpligt med hänsyn till frågans art, den enskildes behov av hjälp och myndighetens verksamhet.[20]

20 Paragrafen syftar till att stärka serviceandan i förvaltningen och att inskärpa vikten av att myndigheterna underlättar allmänhetens kontakter med dem. Sådan service kan som framgått bestå i att t.ex. lämna upplysningar om hur man gör en ansökan eller lämna förslag på enklare sätt för en

I E-delegationens Juridiska vägledning för verksamhetsutveckling inom e-förvaltningen, version 2.0, har detta stöd beskrivits så att en handling i ett eget utrymme hanteras i ett *serviceskede.* Detta skede har beskrivits som ett skyddat förlopp där en användare hanterar uppgifter så att service ges enligt 4 § FL och att ingen annan ges insyn i de uppgifter som behandlas. Av vägledningen framgår också att (ett exemplar av) en handling som finns i en användares eget utrymme inte är föremål för en myndighets handläggning av ett förvaltningsärende. Handlingen är inte att anse som inkommen till myndighet.[21] Denna bedömning har gjorts enligt en sedan länge etablerad myndighetspraxis.

Av 10 § FL följer att en handling anses komma in till en myndighet ”den dag då handlingen … anländer till myndigheten”. En handling på papper har enligt denna regel anlänt till myndigheten när den t.ex. lagts i ett brevinkast till myndighetens lokaler. Frågan om var bland nät och informationssystem en elektronisk handling ska anses inkommen är mera svårgripbar.

En beskrivning av detta gavs redan år 2005 av E-nämnden i en vägledning för hantering av inkommande elektroniska handlingar (e-nämnden 05:02). E-delegationen har anslutit sig till E-nämndens bedömning som innebär att

1. en handling anses ha kommit in när den *nått* den funktion för automatiserad behandling som myndigheten har anvisat för försändelser av aktuellt slag *(anvisat mottagningsställe),*

2. en myndighets mottagningsställe bör utformas så att kvittens sänds när en försändelse har nått myndighetens mottagningsställe och att felmeddelande lämnas om försändelsen helt eller delvis inte har kunnat läsas av myndigheten, och

3. myndigheten löpande bör registrera händelser som kan tyda på fel i någon funktion i myndighetens mottagningsställe.

I denna vägledning görs samma bedömning. När en användare av ett eget utrymme bestämmer sig för att lämna in en handling genom att på ett aktivt och medvetet sätt avsända den till myndighetens elektroniska mottagningsställe blir handling som nått dit inkommen i förvaltningslagens mening.[22]

---

enskild att uppnå det han eller hon önskar. Den kan också bestå i att lämna upplysningar om t.ex. gällande bestämmelser och myndighetens praxis inom ett område, när någon frågar efter det.

21 I E-delegationens Juridiska vägledning för verksamhetsutveckling inom e-förvaltningen, version 2.0, definieras ”Serviceskede” som ett skyddat förlopp där en användare hanterar uppgifter så att (a) service ges enligt 4 § FL, (b) ingen annan ges insyn i de uppgifter som behandlas, (c) det inte sker någon ärendehandläggning, och (d) uppgifterna inte är inkomna enligt 10 § FL.

22 I Förvaltningslagsutredningens betänkande En ny förvaltningslag (SOU 2010:29) föreslås på samma sätt, under rubriken Fastställande av ankomstdagen, att en handling som sänts till ett anvisat elektroniskt mottagningsställe, ska anses ha kommit in när den tagits emot där (18 §). Samtidigt föreslår utredningen en föreskrift om att myndigheten på lämpligt sätt ska anvisa den e-postadress eller annat elektroniskt mottagningsställe dit meddelanden kan sändas och att myndigheten, om inte särskilt hinder möter, ska underrätta avsändaren om ett meddelande har anlänt till det anvisade mottagningsstället och samtidigt ange tidpunkten för mottagandet. Om meddelandet eller bifogat material helt eller delvis inte har kunnat uppfattas, ska avsändaren under-

5.2.2 Service för att motverka fel och brister

Eget utrymme kan utformas så att det inte går att komma vidare för att ge in en handling om en brist konstateras vid den automatiserade service som ges i utrymmet och bristen inte har åtgärdats. Denna service måste emellertid avse procedurer som äger rum innan användaren har sänt iväg handlingen och kunna förenas med användarens berättigade skyddsbehov.

Som framgått av avsnitt 4.3 kan service erbjudas helt automatiserat i användares eget utrymme, utan att handlingar i utrymmet anses vara inkomna till myndigheten. Användaren får stöd för att rätta till brister innan handlingen har sänts till myndigheten. Denna service kan kombineras med tekniska begränsningar som innebär att användaren inte kommer vidare för att skicka in handlingen utan att bristen har åtgärdats.

Som framgått av avsnitt 4.3 och 5.2 blir det inte fråga om en bedömning av om en handling är att anse som inkommen enligt förvaltningslagen utan i vilken omfattning en myndighet ska vara tillgänglig för allmänheten. Vissa allmänna skyldigheter följer av reglerna i 4 och 5 §§ FL om service och tillgänglighet. Enskildas kontakter med myndigheter ska förenklas (4 § FL), myndigheter ska vara tillgängliga elektroniskt (5 §) och enskilda bör hjälpas till rätta så att de använder en lämplig kanal för att ge in en handling (jfr den hjälp som enligt 4 § FL ska ges till den som vänder sig till fel myndighet).

Frågor om automatiserade kontroller har nyligen berörts av regeringen i två lagstiftningsärenden.[23] Så som regeringen redovisat de där införda funktionerna är det möjligt att utforma ett eget utrymme så att det inte går att komma vidare för att ge in en handling, om en brist konstateras vid den automatiserade service som ges i utrymmet och bristen inte har åtgärdats. Begränsningar kan göras eftersom den myndighet som tillhandahåller eget utrymme går utöver den miniminivå som gäller för serviceskyldigheten enligt 5 § FL.

Denna service ska emellertid avse procedurer som äger rum innan användaren har sänt iväg handlingen och utformas så att användarens berättigade behov av skydd tillgodoses. Genom att det t.ex. via e-post går att nå en annan mottagningsfunktion än den för servicetjänsten har användaren möjlighet att ge in en handling via en annan kanal.

---

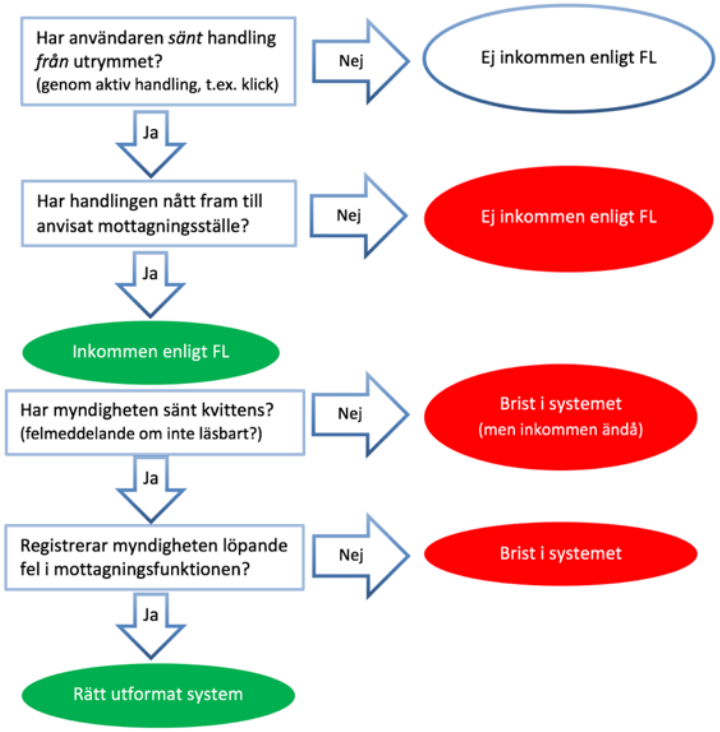
rättas även om det. Se även bl.a. E-nämndens vägledning för hantering av inkommande elektroniska handlingar (e-nämnden 05:02), Furberg i Svensk Juristtidning, Inkommande handlingar – en IT-anpassad tolkning (SvJT 2005, s. 273 ff.) och Förvaltningslagsutredningen (SOU 2010:29, s. 40 och s. 377 ff.).

[23] Se regeringens proposition 2013/14:236 Elektronisk ansökan om lantmäteriförrättning där det anförts att det elektroniska förfarandet motverkar att sökanden av misstag fyller i ansökan fel eller utelämnar viktiga uppgifter, samtidigt som myndighetens behov av att göra kompletteringar minskar (s. 10). Det har vidare, i regeringens proposition 2014/15:10 Förbättringar av husavdragets fakturamodell, redovisats hur kontroller görs av att alla obligatoriska uppgifter är ifyllda och att även en viss formaliakontroll genomförs, samt att en begäran som saknar obligatoriska uppgifter inte kan lämnas innan den har kompletterats. Som exempel på fel, som helt kan undvikas om begäran om utbetalning kommer in via Skatteverkets e-tjänst, har angetts summeringsfel, avsaknad av obligatoriska uppgifter, avsaknad av undertecknande av utföraren och att betalningsdatum angetts som en senare dag än ansökningsdagen (s. 27).

Checklista beträffande inkommande handlingar m.m.

- Vilken service ska myndigheten tillhandahålla genom eget utrymme?
- Finns det en tydlig punkt för att ge in handlingar så att det går att skilja mellan handlingar som finns endast i utrymmet (t.ex. utkast) och kopior av färdigställda handlingar som har sänts iväg till myndigheten?
- Anvisar myndigheten automatiserat ett mottagningsställe som handlingar sändas till och finns det säkra funktioner för att registrera när en handling enligt 10 § FL har kommit in till myndigheten?
- Sänds kvittens från mottagningsfunktionen och underrättas avsändaren, inte bara när överföringen lyckades och handlingen är inkommen, utan även i de fall där ett meddelande inte har gått att läsa?
- Registrerar myndigheten händelser som tyder på att det finns något fel i mottagningsfunktionen och har myndigheten rutiner för att hantera material som nått myndigheten under sådana förhållanden?

Se även följande figur över de huvudfrågor som tillhandahållare av eget utrymme behöver överväga rörande inkommande enligt förvaltningslagen.



5.3 Sekretess och tystnadsplikt

Den som använder ett eget utrymme som en myndighet tillhandahåller behöver veta om det finns risk för att uppgifter i utrymmet röjs för myndigheten eller för någon annan. Här behöver flera frågor klarläggas.

1. Skyddas användaren av utrymmet mot insyn både av utomstående och av myndigheten och dess personal?
2. Kan myndigheten anlita en underleverantör för driften av eget utrymme utan att det leder till ett utlämnande till underleverantören i strid mot OSL eller risk för att uppgifter i utrymmet röjs för utomstående av underleverantören?

5.3.1 Utomstående ska inte ha insyn i eget utrymme

Ett löfte från en myndighet om att skydda uppgifter i eget utrymme mot insyn kan inte hindra ett utlämnande av en handling som visar sig vara allmän och offentlig. Uppgifterna är i så fall inte längre utrymmesinnehavarens privata och utrymmet inte ”eget”.

Som tidigare nämnts blir innehållet i ett korrekt utformat eget utrymme inte att betrakta som allmänna handlingar. En myndighet som tillhandahåller sådant utrymme ska därför inte, till följd av en begäran om utlämnande av allmän handling, behöva ta del av uppgifter i utrymmet för att bedöma om de är offentliga eller sekretessbelagda. Prövningen av den enskildes begäran kan begränsas till att konstatera att handlingarna inte är allmänna och därför inte lämnas ut. Något utlämnande med stöd av 6 kap. 4 eller 5 § OSL kommer inte heller i fråga.

Skulle det visa sig att en myndighet har utformat eget utrymme på fel sätt, så att handlingar i utrymmen har blivit allmänna, är det avgörande om uppgifterna skyddas av sekretess. Gäller absolut sekretess för uppgifter hos en myndighet är de skyddade medan motsatsen gäller om uppgifterna inte alls är sekretessreglerade. Eftersom uppgifter i ett eget utrymme inte hör till den tillhandahållande myndighetens ordinarie verksamhet kan det visa sig att en regel om sekretess för verksamhet som myndigheten bedriver inte omfattar uppgifter i eget utrymme, jfr dock avsnitt 5.3.3 beträffande 40 kap. 5 § OSL och eSams vägledning Outsourcing – en vägledning om sekretess och persondataskydd.

5.3.2 Personalen ska ha tystnadsplikt

Tystnadsplikt för den som sköter driften av it-system där eget utrymme finns kan, beträffande privaträttsliga leverantörer, införas genom avtal. För offentliga funktionärer måste tystnadsplikt däremot följa av bestämmelser i författning.

Det kan som framgått inte uteslutas att personal, som sköter driften av it-system där eget utrymme finns, exempelvis där incidenthantering så kräver, råkar få se informationsinnehåll i ett eget utrymme, trots att arbetsuppgiften inte rör innehållet utan är av endast teknisk art.

Sköts it-driften av en *privaträttslig* leverantör, dvs. hos någon där tryckfrihetsförordningens och offentlighets- och sekretesslagens regler om handlingsoffentlighet och sekretess inte gäller, är det juridiskt möjligt att införa tystnadsplikt som sanktioneras genom avtal och arbetsrättslig reglering. Avtalsreglerad tystnadsplikt blir dessutom fullständig i den meningen att den inte behöver begränsas till vissa slag av uppgifter. När sådana sanktioner – i

förening med de kontroller som behövs – anses ge ett tillräckligt skydd för uppgifter i eget utrymme blir behovet av tystnadsplikt enligt eSams bedömning tillgodosett (se vidare eSams vägledning Outsourcing – en vägledning om sekretess och persondataskydd).[24]

Sköts it-driften i stället av personal *hos en myndighet* är det inte möjligt att *genom avtal* införa ett förbud mot att röja uppgifterna. Tystnadsplikt för offentliga funktionärer regleras i stället i OSL. En sekretessbestämmelse begränsar nämligen inte bara allmänhetens rätt att ta del av uppgifter i allmänna handlingar. Den förbjuder också personal att röja en sekretessbelagd uppgift muntligen eller på något annat sätt (3 kap. 1 § OSL). Det är därför viktigt att klarlägga om sekretess gäller enligt OSL, i de fall it-driften sköts av personal hos en myndighet.[25]

Alla typer av uppgifter omfattas emellertid inte av tystnadsplikt enligt OSL. Innehållet i eget utrymme behöver ändå skyddas mot att röjas av myndighetens personal. Eftersom eget utrymme ska vara utformat så att undantaget enligt 2 kap. 10 § TF blir tillämpligt behöver myndigheten inte, vid en begäran om att få ut en allmän handling som finns i eget utrymme, ta del av innehållet för sin prövning.

Innehållet behöver emellertid också skyddas mot att röjas av myndighetens personal. I första hand ska ett sådant skydd införas så att personalen *inte kan* och – beträffande någon enstaka person med särskilt hög behörighet – *inte får* bereda sig tillgång till uppgifter i eget utrymme. Bereder sig någon ändå olovligen tillgång till sådana uppgifter ska regler, avtal och tekniska begränsningar så långt möjligt utformas så att det kan dömas till ansvar om myndighetens personal missbrukar sin tillgång till sådant material.

För eget utrymme som avses användas för sådana uppgifter att tystnadsplikt inte gäller ska särskilda åtgärder vidtas så att de som sköter driften av eget utrymme inte råkar få syn på innehållet i något utrymme; jfr att en vaktmästare som har huvudnyckel till en lägenhet och går in för att stoppa ett vatten-

---

24 Se även Myndigheten för samhällsskydd och beredskaps skrift Vägledning – informationssäkerhet i upphandling.

25 När det övervägs om eget utrymme har utformats så att det får anses vara eget även i detta avseende behöver det uppmärksammas att tystnadsplikten enligt OSL bara i vissa fall *har företräde* framför rätten att meddela och offentliggöra uppgifter. Detta kan närmare beskrivas så att en bestämmelse om sekretess ofta för med sig en begränsning även av yttrandefriheten enligt regeringsformen. Rätten att meddela och offentliggöra uppgifter har enligt huvudregeln företräde framför den tystnadsplikt som följer av en sekretessbestämmelse, men den har aldrig företräde framför den sekretess för handling som gäller enligt samma bestämmelse (se 1 kap. 1 § TF och 1 kap. 1 och 2 §§ yttrandefrihetsgrundlagen, i det följande ”YGL”, 7 kap. 3 § första stycket 2 och 5 § TF och 5 kap. 1 § första stycket och 3 § 2 YGL). – I andra fall kan det däremot vara tillåtet för en befattningshavare som administrerar eget utrymme och har fått del av en uppgift som finns där att lämna uppgiften muntligen till en journalist eller att själv publicera den, trots att uppgiften är sekretessbelagd. Det är dock aldrig tillåtet att med stöd av meddelarfriheten lämna ut den allmänna handling som den sekretessbelagda uppgiften framgår av. Beträffande exemplen där sekretess gäller enligt 27 kap. 1 § eller 40 kap. 5 § OSL är meddelarfriheten helt inskränkt enligt 27 kap. 10 § och 40 kap. 8 § OSL.

läckage får syn på och läser t.ex. ett utkast till en inlaga i ett ärende. När sådana begränsningar har införts återstår endast ett fåtal ”lovliga” fall där den som sköter driften av eget utrymme utför en uppgift så som att rätta ett tekniskt fel eller att åtgärda en informationssäkerhetsrelaterad brist och då råkar få syn på en uppgift i ett eget utrymme. I så fall finns ingen avsikt att ta del av uppgiften.

Trots en förfrågan hos flera av de myndigheter som tillhandahåller eget utrymme har eSam inte kunnat finna exempel på att information kommit till en befattningshavares kännedom på detta sätt. För fullständighetens skull och för att säkerställa att tillräckliga regler och tekniska skydd införs, bör dock den som ska tillhandahålla eget utrymme överväga regleringen även i denna del (jfr SOU 2014:39).

5.3.3 Tystnadsplikt kan gälla enligt 40 kap. 5 § OSL

En tystnadsplikt som är absolut kan följa av en bestämmelse i OSL om sekretess i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning av personuppgifter som avses i personuppgiftslagen för uppgift om en enskilds personliga eller ekonomiska förhållanden. Eftersom det regelmässigt torde förekomma åtminstone någon personuppgift i eget utrymme, innebär detta att alla uppgifter som finns i utrymmet och som rör användarens eller annan enskilds personliga eller ekonomiska förhållanden omfattas av tystnadsplikten.

Enligt 40 kap. 5 § OSL gäller sekretess i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning av personuppgifter som avses i personuppgiftslagen för uppgift om en enskilds personliga eller ekonomiska förhållanden. Denna tystnadsplikt är absolut, vilket innebär att uppgifter som omfattas av sekretessen ska hemlighållas utan någon skadeprövning. Bestämmelsen är av direkt relevans avseende skyddet för uppgifter i eget utrymme. E-delegationen har i ett betänkande, SOU 2014:39, gjort bedömningen att sekretessens föremål enligt 40 kap. 5 § OSL är begränsat till att endast avse personuppgifter. Mot denna bakgrund har E-delegationen dragit slutsatsen att bestämmelsen inte erbjuder något sekretesskydd i fråga om sådana uppgifter om enskilda som inte utgör personuppgifter i personuppgiftslagens mening, dvs. uppgifter om företag. E-delegationen har därför föreslagit en ändring av paragrafen. Förslaget har inte lett till lagstiftning.

E-delegationens tolkning av bestämmelsen i 40 kap. 5 § OSL är emellertid inte självklar. Mycket talar för att avgränsningen till ”personuppgift” i stället avser bestämmelsens räckvidd, dvs. i vilken verksamhet som bestämmelsen är tillämplig. En sådan tolkning innebär att sekretessen gäller i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning av personuppgifter.

Bestämmelsen är alltså inte tillämplig i alla typer av bearbetnings- eller lagringsverksamhet för annans räkning, utan bara i sådan verksamhet som omfattar bearbetning eller lagring av material där personuppgifter förekommer. I sådan verksamhet gäller dock absolut sekretess för alla uppgifter om enskilds personliga och ekonomiska förhållanden, dvs. även rörande bolag och enskilda näringsidkare. Eftersom det regelmässigt torde förekomma åt-

minstone någon personuppgift i eget utrymme, innebär detta enligt eSams bedömning att alla uppgifter som finns i utrymmet och som rör användarens eller annan enskilds personliga eller ekonomiska förhållanden skyddas av sekretess, se vidare eSams vägledning Outsourcing – en vägledning om sekretess och persondataskydd.

5.3.4 Underleverantör för eget utrymme

I en särskild vägledning har eSam närmare beskrivit och redovisat lämpliga åtgärder rörande sekretess vid outsourcing.

Beträffande frågan om en myndighet kan anlita en underleverantör för driften av eget utrymme utan att det leder till ett utlämnande till underleverantören i strid mot OSL eller risker för att uppgifter i utrymmet röjs för utomstående av underleverantören hänvisas till eSams vägledning Outsourcing – en vägledning om sekretess och persondataskydd. Se även eSams rättsliga uttalande Röjandebegreppet enligt offentlighets- och sekretesslagen.

I detta sammanhang bör också beaktas att de särskilda krav som aktörerna behöver uppfylla vid outsourcing måste klargöras och tas in i avtal och annan reglering redan när tjänsterna utvecklas och upphandlas.[26]

Checklista beträffande sekretess och tystnadsplikt

- Finns det risk för att innehållet i eget utrymme röjs för utomstående till följd av att uppgifter där blir att anse som allmän handling och att uppgifterna inte är sekretessbelagda hos tillhandahållaren av utrymmet?
- Gäller tystnadsplikt för tillhandahållande myndighets personal?
- Gäller tystnadsplikt för myndighetens eventuella underleverantörer?
- Är tystnadsplikten författningsreglerad och sanktionerad genom straffansvar eller kan avtalsreglerad tystnadsplikt i förening med arbetsrättsligt ansvar och en skyldighet att betala skadestånd räcka?
- Gäller sekretess enligt 40 kap. 5 § OSL för alla uppgifter i utrymmet?

Se vidare eSams vägledning Outsourcing – en vägledning om sekretess och persondataskydd.

[26] Detta gäller inte minst säkerhetskrav och skyldigheter rörande obligatorisk it-incidentrapportering. Ytterligare stöd för arbetet med att omhänderta säkerhetsbehov ges av Myndigheten för samhällsskydd och beredskap i Vägledning – informationssäkerhet i upphandling

5.4 Bevarande och gallring

Eget utrymme ska vara utformat så att handlingar som finns i utrymmet inte blir allmänna. Arkivförfattningarna blir därför inte tillämpliga. Skulle ett fel i eller ett brottsligt angrepp mot ett utrymme leda till att handlingar som finns där blir allmänna behöver åtgärder vidtas för att handlingarna inte ska kunna begäras ut. Handlingar som felaktigt blivit allmänna till följd av ett tekniskt misstag eller ett brottsligt angrepp som rör eget utrymme torde kunna gallras.

En myndighet som tillhandahåller eget utrymme behöver genom noggrant utformade regler och tekniska begränsningar se till att otillåten lagring av uppgifter i eget utrymme motverkas.

Av arkivlagen (1990:782) följer att myndigheternas arkiv ska bevaras, hållas ordnade och vårdas så att de tillgodoser rätten att ta del av allmänna handlingar, behovet av information för rättskipningen och förvaltningen, och forskningens behov. Sådana handlingar ska finnas kvar i ursprungligt skick. Alla åtgärder som innebär förstöring av allmänna handlingar och uppgifter i allmänna handlingar eller annan informationsförlust utgör gallring. Även t.ex. skärmbilder som ges in till en myndighets hjälptjänst omfattas av denna reglering. – Arkivet består dock bara av myndighetens allmänna handlingar.

Har en handling blivit allmän får gallring ske bara om åtgärden är tillåten enligt särskilda gallringsföreskrifter i lag eller förordning eller i enlighet med föreskrifter eller beslut av Riksarkivet.[27] För kommuner och landsting framgår det inte av arkivlagen vem som ska besluta om gallring vilket innebär att nämnderna, som verksamhetsansvariga och ansvariga för vården av sina handlingar, själva beslutar om gallring av sina handlingar, om inte fullmäktige beslutat att arkivmyndigheten ska ha detta ansvar.[28] Här kan också noteras att en allmän handling, enligt 5 kap. 1 § OSL, varken behöver registreras eller hållas ordnad om det är uppenbart att den är av ringa betydelse för myndighetens verksamhet.

Riksarkivet har utfärdat generella gallringsföreskrifter för handlingar av tillfällig eller ringa betydelse för myndighetens verksamhet. Enligt 7 § Riksarkivets föreskrifter och allmänna råd om gallring av handlingar av tillfällig eller ringa betydelse (RA-FS 1991:6; ändrad genom RA-FS 1997:6) får sådan gallring ske endast under förutsättning att allmänhetens rätt till insyn inte åsidosätts och att handlingarna bedöms sakna värde för rättskipning, förvaltning och forskning. För kommuner och landsting gäller som framgått särskilda regler.

---

[27] Se 10 § arkivlagen (1990:782) och 14 § arkivförordningen (1991:446). Handlingar som skickas från eget utrymme till myndighet behöver uppfylla Riksarkivets föreskrifter och allmänna råd om tekniska krav för elektroniska handlingar (RA-FS 2009:2).

[28] Se vidare Arkivlagen – En kommentar- U Geijer m.fl. , Norstedts gula bibl., 2013, s. 194.

Av myndighetens tillämpningsbeslut rörande gallring av handlingar av tillfällig och ringa betydelse bör således framgå att även handlingar av detta slag får gallras. En bedömning får emellertid göras utifrån förutsättningarna för den enskilda tjänsten. För kommuner och landsting gäller som framgått särskilda regler enligt vilka motsvarande beslut kan fattas inom det området.

Något insynsintresse enligt TF kan inte rimligen finnas i enskildas utkast och liknande material som de har i ett eget utrymme. I E-delegationens Juridiska vägledning för verksamhetsutveckling inom e-förvaltningen, version 2.0 har omedelbar gallring beskrivits så att åtgärden kan tillgodose enskildas befogade förväntningar på att andra inte ska ges tillgång till visst material.[29]

Skulle i något undantagsfall t.ex. ett tekniskt fel i eller ett brottsligt angrepp mot ett eget utrymme leda till att handlingar där har råkat bli allmänna behöver myndigheten vidta åtgärder för att skydda användaren. Eftersom eget utrymme tillhandahålls som användarens eget och särskilt har utformats för att ingen annan ska få ta del av det som finns där kan det enligt eSams bedömning antas att hinder normalt inte finns mot att myndigheten beslutar att gallring får ske av handlingar som råkat bli allmänna.[30]

När handlingar i eget utrymme inte är allmänna och arkivförfattningarna således inte gäller blir det i stället nödvändigt att *rensa bort* visst material. Myndigheter får som framgått tillhandahålla eget utrymme endast om hanteringen ryms inom ramen för myndighetens uppdrag, som framgår av myndighetens instruktion, andra författningar, regleringsbrev eller andra särskilda beslut. Till en myndighets uppdrag hör inte att tillhandahålla en allmän lagringsplats för utrymmesinnehavarens bruk.

Begränsningar behöver således införas så att den tjänst en myndighet tillhandahåller faller inom ramen för myndighetens uppgifter. Vidare krävs begränsningar från informationssäkerhetssynpunkt och för att personuppgifter inte ska behandlas längre än vad som är nödvändigt för ändamålet. Angivet ändamål blir här av avgörande betydelse för hur utrymmet ska få användas. En myndighet som tillhandahåller eget utrymme bör därför genom noggrant utformade tekniska begränsningar och juridiskt bindande regler se till att otillåten lagring förhindras eller i vart fall motverkas. Dessa begränsningar behöver knytas till fungerande sanktioner, t.ex. genom regler om rätt för tillhandahållande myndighet att stänga av möjligheten för den enskilde att logga in i sitt utrymme eller att avsluta ett utrymme som används i strid med gällande villkor och att rensa bort de uppgifter som finns där.

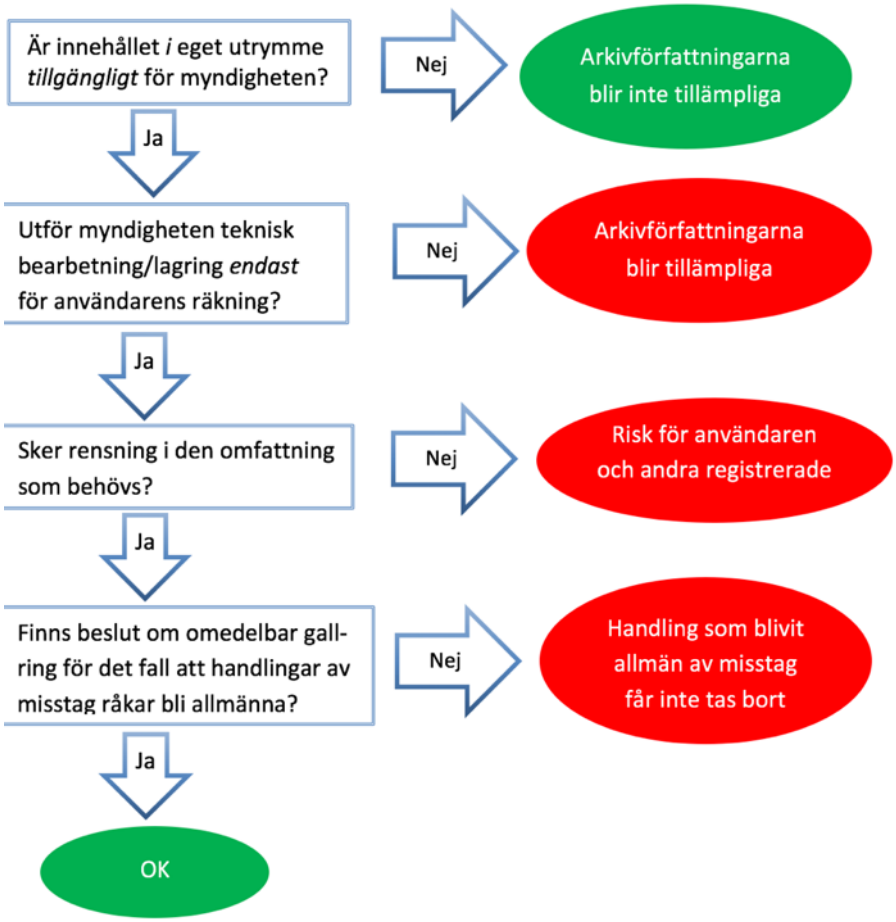
Checklista beträffande bevarande och gallring

[29] Liknande frågor uppkommer om uppgifter görs tillgängliga för en myndighet i en hjälptjänst och när uppgifter samlas in av myndighet för att sammanställas innan de lämnas ut till eget utrymme.

[30] JO har inte funnit anledning att kritisera en myndighet som – med stöd av ett beslut om gallring av handlingar av tillfällig eller ringa betydelse – raderat ett otillåtet register över samtliga e-postmeddelanden som medarbetare inom myndigheten tagit emot och skickat under en viss tidsperiod (JO:s beslut den 2 Mars 2016, dnr. 6696-2014).

- Blir arkivförfattningarna tillämpliga på innehållet i eget utrymme?
- Finns gallringsbeslut för den händelse att handlingar i eget utrymme skulle råka bli allmänna?
- Finns avtalsvillkor eller andra regler för användare för att utrymmet ska rensas i rimlig omfattning och olämplig användning hindras?

Se även följande figur över de huvudfrågor som tillhandahållare av eget utrymme behöver överväga rörande bevarande och gallring.



5.5 Skyddet för personuppgifter

Myndigheten ska vid utformningen och driften av eget utrymme beakta integritetsskyddslagstiftningen.

Enligt 3 § PuL utgör varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter en behandling av personuppgifter. Även teknisk bearbetning eller teknisk lagring av personuppgifter utgör behandlingsåtgärder i personuppgiftslagens mening. Varje sådan behandling av personuppgifter måste ske i enlighet med personuppgiftslagens och tillämpliga registerförfattningars bestämmelser om under vilka omständigheter en behandling är laglig.

Det är den personuppgiftsansvarige som bär det juridiska ansvaret för att integritetsskyddet upprätthålls. Denna skyldighet rör bl.a. uppgifternas kvalitet i sammanhanget, t.ex. att behandlingen av en viss typ av personuppgift är laglig, korrekt och nödvändig. Det är alltid den personuppgiftsansvarige som är skyldig att ersätta den registrerade för en skada eller kränkning som en otillåten behandling har orsakat. Dessutom är det den personuppgiftansvariges skyldighet att tillgodose den registrerades rätt till information, rättning, utplåning eller blockering.

En viktig del av personuppgiftsansvaret är att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Beslutet om vilka åtgärder som ska vidtas kan visserligen delegeras till ett personuppgiftsbiträde, men ansvaret gentemot den registrerade ligger ändå hos den personuppgiftsansvarige. Den personuppgiftsansvarige ansvarar också för att det inte sker någon otillåten överföring av personuppgifter till tredje land. Slutligen är den personuppgiftsansvarige central för personuppgiftslagens bestämmelser om anmälan till och tillsyn av Datainspektionen.

5.5.1 Vem är personuppgiftsansvarig?

Frågan om i vilken mån myndigheten är personuppgiftsansvarig för de behandlingar av personuppgifter som sker i eget utrymme har varit föremål för diskussion under flera år. Det finns än så länge inte någon vägledande dom på området och rättsläget måste därmed anses vara oklart. Nedan beskrivs tre alternativa synsätt.

Enligt E-delegationens Juridiska vägledning för verksamhetsutveckling inom e-förvaltningen, version 2.0, är den myndighet som tillhandahåller eget utrymme endast personuppgiftsansvarig för den drift- och säkerhetsrelaterade information som avser utrymmet och i övrigt för att de personuppgifter som behandlas i utrymmet är omgärdade av adekvata säkerhetsåtgärder. Däremot är tillhandahållaren, enligt E-delegationen, inte personuppgiftsansvarig för den nyttoinformation som användaren själv för in i sitt utrymme och inte heller för sådana uppgifter som myndigheten har expedierat dit.

Av en fotnot till E-delegationens vägledning framgår att Datainspektionen inte delar E-delegationens bedömning. Inspektionen menar att personuppgiftsansvaret antingen regleras i registerförfattning eller bestäms utifrån vem som bestämmer ändamål och medel med behandlingen och att detta normalt leder till att myndigheter har personuppgiftsansvar för all behandling av personuppgifter i egna utrymmen, det vill säga även för det som av E-delegationen benämns nyttoinformation.

Om två parter tillsammans bestämmer ändamål och medel med behandlingen är båda dessa parter personuppgiftsansvariga enligt 3 § PuL. Ett sådant gemensamt ansvar skulle kunna övervägas avseende egna utrymmen som

disponeras av juridiska personer eller enskilda näringsidkare.[31] Myndigheten och respektive användare kan då komma överens om en effektiv fördelning av de olika skyldigheter som följer med personuppgiftsansvaret. Denna fördelning måste redovisas öppet och tydligt.

Närmare om grunderna för Datainspektionens bedömning

Reglerna kring personuppgiftsbehandling har ett annat syfte och en annan konstruktion än bestämmelserna om allmänna handlingar. Skyddet för personuppgifter har sitt ursprung i rätten till privatliv och i artikel 8 i EU:s stadga om de grundläggande rättigheterna uttrycks det direkt att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Skyddet gör sig med andra ord gällande när någon vill behandla någon annans personuppgifter.

Den som behandlar uppgifter i sin verksamhet kan göra det antingen som personuppgiftsansvarig eller som personuppgiftsbiträde. Personuppgiftsansvarig är den som bestämt ändamål och medel för att personuppgiftsbehandlingen eller den som i författning pekas ut som personuppgiftsansvarig. Den personuppgiftsansvarige måste ha ett rättsligt stöd för behandlingen. . Enskilda fysiska personer som behandlar personuppgifter för privatbruk är undantagna från kravet på rättsligt stöd. Det undantaget kan inte åberopas av juridiska personer. Personuppgiftsbiträdet behandlar personuppgifter i sin verksamhet på uppdrag av en personuppgiftsansvarig. Ett personuppgiftsbiträde får inte självständigt vidta några åtgärder med uppgifterna, utan kan endast behandla dem i enlighet med vad som angetts i det avtal som ska upprättas mellan den personuppgiftsansvarige och personuppgiftsbiträdet. Den personuppgiftsansvarige är även ansvarig och måste ha ett rättsligt stöd för den behandling av personuppgifter som personuppgiftsbiträdet utför inom uppdragets ram.

Personuppgiftsansvaret omfattar de personuppgifter som behandlas och med behandling avses alla åtgärder som vidtas i fråga om personuppgifterna t.ex. att uppgifterna samlas in, lagras, bearbetas, sprids, sammanställs, organiseras m.m. Vid myndigheters informationshantering måste både reglerna gällande allmänna handlingar och dataskyddsbestämmelserna beaktas, men de ska inte tolkas i ljuset av varandra utan måste analyseras var för sig.

Någon motsvarighet till TF 2:10 finns inte i dataskyddsbestämmelserna och följaktligen finns det inte några särskilda regler för personuppgiftsbehandling i s.k. egna utrymmen. Myndigheter som tillhandahåller egna utrymmen gör det ofta i ett servicesyfte, t.ex. för att kunna ge medborgare enkel tillgång till uppgifter som rör den enskilde medborgaren eller för att medborgaren själv ska kunna lämna uppgifter till myndigheten. Denna service måste

[31] Enligt 6 § PuL gäller personuppgiftslagen inte för sådan behandling av personuppgifter som en fysisk person utför som ett led i en verksamhet av rent privat natur. En privatperson kan således varken vara ensamt eller gemensamt personuppgiftsansvarig.

ta sin utgångspunkt i den verksamhet som myndigheten är ålagd att utföra, se 4 § förvaltningslagen (1986:223). Det är myndigheten som avgör att det egna utrymmet ska inrättas, vad det ska ha för funktion, för vem och hur det ska utformas. Det är således, enligt Datainspektionens uppfattning, myndigheten som bestämmer ändamål och medel och som därmed är personuppgiftsansvarig för personuppgiftsbehandlingen. Regleras personuppgiftsansvaret i en särskild författning och den omfattar den behandling av personuppgifter som sker i det egna utrymmet blir resultatet ofta detsamma, eftersom det ofta är myndigheten som utpekas som ansvarig i dem. Personuppgiftsansvaret påverkas inte av om myndigheten tar del av informationen som finns i det egna utrymmet eller inte.

Med personuppgiftsansvaret följer skyldigheter för den ansvarige såsom exempelvis att informera den registrerade, att skydda uppgifterna från obehörig åtkomst, att tillse att inte fler uppgifter än nödvändigt behandlas och att behandlingen inte sker längre tid än nödvändigt. Den personuppgiftsansvarige måste också respektera den registrerades rättigheter såsom rätt till rättelse, rätt att få uppgifter raderade, rätt att få del av vilka uppgifter som finns registrerade genom s.k. registerutdrag osv. Vidare måste rättigheterna för de personer vars uppgifter kan komma att behandlas utan att de själva har insyn i det egna utrymmet beaktas. Myndigheten måste, innan en tjänst i form av eget utrymme inrättas, analysera så att det finns rättsligt stöd för tjänsten och att myndigheten har förmåga att uppfylla de skyldigheter och rättigheter som följer av dataskyddsbestämmelserna gällande samtliga som registreras i tjänsten.

5.5.2 Hur bör myndigheten utöva sitt ansvar?

Även om det måste anses vara oklart var de yttre gränserna för myndighetens personuppgiftsansvar avseende eget utrymme går, står det klart att den tillhandahållande myndigheten måste beakta integritetsskyddslagstiftningen vid utformningen och driften av tjänsten och vidta vissa åtgärder. Myndighetens ansvar ska dock utövas på ett systematiskt och övergripande plan och får inte inkräkta på utrymmets karaktär som användarens ”eget”.

1. En myndighet kan bara tillhandahålla eget utrymme för sådan behandling av personuppgifter som är tillåten enligt den dataskyddslagstiftning som gäller för myndigheten.[32] Myndighetens tekniska bearbetning och lagring av personuppgifterna i användarens utrymme skulle annars vara otillåten.

2. Myndigheten måste utforma utrymmet och instruktionerna till användaren så att det blir tydligt för vilket ändamål behandling av per-

[32] När en registerförfattning gäller för en myndighet som tillhandahåller eget utrymme behöver författningens tillämpningsområde övervägas. Myndigheten måste bedöma om registerförfattningen eller personuppgiftslagen ska tillämpas

sonuppgifter får ske samt vilka slags personuppgifter som är relevanta för ändamålet och därmed får behandlas i utrymmet.

3. Myndigheten måste tekniskt begränsa lagringstiden så att personuppgifter inte bevaras i utrymmet under längre tid än nödvändigt.

4. Myndigheten måste vidta lämpliga säkerhetsåtgärder för att skydda de uppgifter som behandlas i utrymmet. Detta gäller såväl funktioner för identifiering och kontroll av behörighet som åtgärder för att skydda utrymmet genom brandväggar, intrångsdetekteringssystem och liknande.

5. Myndigheten måste säkerställa att ingen otillåten överföring till tredje land sker avseende personuppgifter i eget utrymme, t.ex. genom användning av vissa s.k. molntjänster.

6. Systemet ska inte tillåta sökningar som visar i vilka användares utrymmen som en viss personuppgift förekommer. Om sådana sökmöjligheter finns måste användarna på förhand informeras om att s.k. registerutdrag kan komma att lämnas ut till registrerade som begär ett sådant.

De ovan beskrivna åtgärderna kan vidtas utan att myndigheten behöver ta del av innehållet i någon användares utrymme. Myndigheten kan därmed säkerställa en ansvarsfull personuppgiftsbehandling utan att utrymmets karaktär som ”eget” påverkas. Vidare ska myndigheten inte vidta några andra åtgärder med handlingarna i utrymmet än att tekniskt bearbeta och tekniskt lagra dem för användarens räkning. Myndighetens personuppgiftsansvar påverkar därmed inte den tidigare redovisade bedömningen att handlingar i ett korrekt utformat eget utrymme omfattas av undantaget i 2 kap. 10 § första stycket TF och därmed inte utgör allmänna handlingar.

Checklista beträffande persondataskydd

- o Bestäms personuppgiftsansvar för behandlingar av personuppgifter i ett eget utrymme av en registerförfattning?
- o Kan privatundantaget bli tillämpligt vid de personuppgiftsbehandlingar som avses ske i utrymmet?
- o Behöver myndigheten, om den är personuppgiftsansvarig för utrymmet, bereda sig tillgång till användarens uppgifter i utrymmet?

5.6 Tillhandahållande myndighets uppdrag

Serviceverksamhet genom eget utrymme ryms inom en myndighets uppdrag om verksamheten faller inom den yttre ram som anges vara myndighetens grundläggande uppgifter och befogenheter. Aktiviteter helt vid sidan av det i författning angivna uppdraget är däremot inte tillåtna.

En myndighets serviceverksamhet består inte bara av aktiviteter som direkt går att identifiera som utförande av uppgifter och befogenheter som framgår av författning, regleringsbrev eller särskilda regeringsbeslut. Verksamheten måste emellertid begränsas till vad som ligger inom myndighetens grundläggande uppgifter och befogenheter.[33]

Serviceverksamhet genom eget utrymme för att förenkla för enskilda att t.ex. upprätta skattedeklaration eller att registrera företag får anses rymmas inom berörd myndighets uppdrag, utan särskild tillåtande reglering. Hjälpen faller inom den yttre ram som anges genom myndighetens grundläggande uppgifter och befogenheter. Aktiviteter som ligger helt vid sidan av det i författning angivna uppdraget är däremot inte tillåtna. Ska sådan verksamhet bedrivas av en myndighet krävs författningsändringar.[34]

5.7 Reglering av eget utrymme

En myndighet som tillhandahåller eget utrymme bör när det inte finns någon offentligrättslig reglering av området reglera mellanhavandet med användare genom avtal. Denna bedömning gäller även om myndigheten har utkontrakterat driften av eget utrymme.

När en myndighet tillhandahåller eget utrymme bör detta mellanhavande regleras mellan myndigheten och användaren av utrymmet. Sådana regler kan ges i lag, förordning eller myndighetsföreskrifter eller genom villkor i förvaltningsbeslut för enskilda fall. Mellanhavandet regleras i så fall offentligrättsligt. Regler kan emellertid också införas genom avtal.

Eget utrymme har nu fått en omfattande spridning, med privaträttsliga handelsmönster och avtalskonstruktioner som förebild. Vad som tillhandahålls är dock endast en teknisk plattform med automatiserade funktioner för en-

---

[33] Någon form av förankring i lag eller annan författning behövs för all verksamhet som bedrivs av en myndighet, även sådan som inte uttryckligen tar sikte på beslutsfattande i klassisk mening. Risken för övertramp har ökat i och med att klassisk förvaltning allt mer kommit att sammanblandas med informationsuppgifter och mera kundrelaterade aktiviteter (SOU 2010:29 s. 24 och 147). Bemyndigandet får i ett sådant fall anses implicit framgå av uppgiftsbeskrivningen. Vad som hindras av en på så sätt uppfattad legalitetsprincip är aktiviteter som ligger helt vid sidan av det i författning angivna uppdraget. Se vidare SOU 2015:39 s. 277, 280 och 288.

[34] Service som har direkt bäring på en viss ärendekategori som hör hemma inom myndighetens traditionella kärnverksamhet regleras normalt inte särskilt i lag eller förordning medan service av helt annat slag, t.ex. den som Skatteverket tillhandahåller genom mina meddelanden eller E-legitimationsnämnden med avseende på elektronisk legitimering och underskrift, har stöd i uppdrag som följer av särskilda bestämmelser i förordning.

skildas egen hantering av uppgifter. Dessa tjänster är begränsade till funktioner som lika gärna kan tillhandahållas genom en privaträttslig aktör. Inget förvaltningsärende har anhängiggjorts.

Så länge det inte finns någon offentligrättslig reglering av denna hantering finns enligt eSams bedömning inte hinder mot att införa regler genom avtal om användningen av eget utrymme. En myndighet som tillhandahåller eget utrymme bör således reglera dessa mellanhavanden genom avtal. Denna bedömning gäller även om myndigheten har utkontrakterat driften av den tjänst som myndigheten tillhandahåller åt enskilda.

Checklista beträffande regler i avtal eller författning

- Får myndigheten tillhandahålla planerade funktioner för eget utrymme utan att detta särskilt föreskrivits i förordning?
- Ska myndigheten reglera tillhandahållandet av eget utrymme genom avtal med användare, genom beslut för enskilda fall eller genom föreskrifter?
- Vilka regler behövs för att skydda myndigheter och enskilda?

6. Praktisk utformning

6.1 Det behövs regler

Hittills har särskilda föreskrifter för eget utrymme och avtalsvillkor om hur användare får bruka utrymmet inte förekommit. Tekniska begränsningar och allmänna beskrivningar har ansetts tillräckliga. Något missbruk genom att användare hanterat sitt utrymme för andra syften än de avsedda verkar inte heller ha förekommit, i vart fall inte i sådan omfattning att det kommit till myndigheternas kännedom. De kända hoten verkar istället ha varit att någon vilseleder en användare i syfte att olovligen bereda sig tillgång till eller annars missbruka användarens utrymme. I samband med att användningsområdet för eget utrymme växer och antalet användare ökar kan det dock antas att hotbilden förändras.

Eget utrymme har nu fått en sådan spridning och en så central roll i myndigheternas arbete för att tillhandahålla säkra och funktionella elektroniska tjänster att hanteringen bör göras tydlig och regleras så att missbruk av eget utrymme kan undgås på sikt och att skyddet för användare kan säkerställas. Som framgått kan eget utrymme emellertid erbjuda vitt skilda funktioner (se kap. 2) och beröra olika regelverk utifrån delvis motstående skyddsintressen (se kap. 5). En vägledning för eget utrymme behöver därför ha en konkret och praktisk inriktning så att berörda aktörers behov av skydd säkerställs. eSam har därför utgått från vilka regler som kan behövas i form av föreskrifter eller avtalsvillkor.

6.2 Inledande åtgärder

6.2.1 Klarlägg vissa grundläggande frågor

Efter att en myndighet som planerar att tillhandahålla eget utrymme *har*

- *utrett*
  - om det faller inom myndighetens uppdrag att tillhandahålla utrymmen av berört slag (se avsnitt 5.6),
  - att hinder inte finns mot att reglera mellanhavandet med användaren genom avtal (se avsnitt 5.7),
  - vilken information som ska behandlas och hur den ska skyddas (se avsnitt 3.2), och
  - vilka regler som behöver införas (se avsnitt 6.2-6.5), och
- *bestämt* en sådan grundläggande utformning att utrymmena kan uppfylla
  - rekvisiten i centrala rättsregler (se avsnitt 4.1 och 5.1-5.5), och
  - användarnas förväntningar på att ingen annan tar del av uppgifter i användarens utrymme eller annars missbrukar det (se avsnitt 4.2),

kvarstår att närmare *bestämma*

- vilka automatiserade servicefunktioner som ska tillhandahållas,

- vilken eller vilka service- och presentationstjänster som utrymmet ska ge stöd för, och
- hur regler för utrymmet ska bli juridiskt bindande för berörda aktörer.

6.2.2 Beskriv tjänsten

Utrymmet bör beskrivas på en webbsida som är knuten till den webbsida där användare av eget utrymme legitimerar sig för tillträde till tjänsten.

När regler om tjänster ges genom lag, förordning eller myndighetsföreskrifter är det naturligt att tjänsten översiktligt beskrivs i författningen.[35] Vilken eller vilka av en myndighets tjänster som ska stödjas och vilka automatiserade servicefunktioner ett eget utrymme närmare ska tillhandahålla föreskrivs emellertid inte i författning. Inte heller när den tjänst som en myndighet tillhandahåller regleras genom avtal brukar reglerna – här användarvillkoren – innefatta någon beskrivning av vilken eller vilka service- eller presentationstjänster som utrymmet ska stödja och vilka automatiserade servicefunktioner som utrymmet ska erbjuda.

En redovisning av eget utrymme som en viss myndighet tillhandahåller behöver emellertid finnas i någon form, särskilt som ett sådant utrymme kan utformas på många olika sätt. Det är således, oberoende av om ett eget utrymme regleras genom författning eller avtal, lämpligt att tillhandahålla en beskrivning av tjänsten. Den bör ges på *en webbsida,* med en tydlig länk från den webbsida som först möter en användare som ska logga in för att använda den servicetjänst eller en presentationstjänst som utrymmet stödjer.

6.2.3 Ange de servicefunktioner myndigheten tillhandahåller

Beskrivningen av eget utrymme bör anpassas till de servicefunktioner som myndigheten tillhandahåller och samordnas med hur andra myndigheter beskriver eget utrymme.

Beskrivningen av vad en myndighet tillhandahåller i form av eget utrymme bör samordnas på myndighetsområdet så att användare enkelt kan förstå informationen, känna igen sig från myndighet till myndighet och jämföra vad som erbjuds. Dessutom behöver beskrivningens omfattning och inriktning anpassas till förutsättningarna i det enskilda fallet.

När eget utrymme inte medger mellanlagring för att fortsätta att använda utrymmet senare och endast innehåller hårt styrda fält för att registrera vissa förutbestämda uppgifter är behovet begränsat av att informera om funktioner och användning. Risken för missbruk av utrymmet kan också bli försumbar. Ingen annan än den användare som registrerar uppgifter under en kort

[35] Se t.ex. den i avsnitt 2.2 nämnda 5 § förordningen om statliga myndigheters elektroniska informationsutbyte, där det anges vilka som får anslutas till Mina meddelanden och vad tjänsten i huvudsak ska innefatta.

stund ser det som skrivs och när användaren kopplar ner sig försvinner utrymmet och de uppgifter som har funnits där.

För sådana utrymmen är det viktigt att användaren få tydlig information om att det inte går att logga ut och senare hämta upp det som har registrerats.

Situationen blir en annan när en myndighet tillhandahåller alla de funktioner som beskrivits ovan, med fält för fri text samt möjligheter att hämta och bevara uppgifter under viss tid och att lämna fullmakt för annan att bruka utrymmet för användarens räkning, med de risker detta kan innebära för registrering, ändring och utbyte av uppgifter på sätt som myndigheten inte har avsett. Här kan också förekomma ärenden där ansökningsavgift utgår. För att undgå komplikationer i denna del, med traditionella förelägganden om att betala avgiften och avvisning när betalning inte kommer in, kan funktioner för elektronisk betalning ha införts som ett led i proceduren för att kunna sända iväg handlingen. I dessa fall blir behovet större av analyser och beskrivningar av utrymmet och regler för användningen.

En beskrivning kan behöva innehålla information bl.a. om att

- myndigheten inte får ta del av den information som användaren har i utrymmet,
- uppgifter som förifyllts måste kontrolleras av användaren innan handlingen ges in,
- automatiserade kontroller utförs bl.a. av att uppgifter räknas samman rätt och att de stämmer med uppgifter i ett offentligt register,
- automatiserade kontroller utförs av att elektroniska underskrifter har producerats korrekt,
- krav på innehåll och form ställs,
- endast vissa typer av information tillåts,
- adressering sker automatiserat till ett anvisat elektroniskt mottagningsställe där myndigheten tar emot handlingar av berört slag och att en handling anses vara inkommen enligt förvaltningslagen först när den har nått fram till mottagningsstället,
- användaren för vissa fall kan hämta uppgifter från annan direkt till sitt eget utrymme (egen hämtning) och automatiserat kan sammanställa uppgifter som förts in i utrymmet (egen visning),
- det är förbjudet (straffbart) att lämna ut sin e-legitimation till någon annan i syfte att låta denne logga in – och möjligen även skriva under elektroniskt – i användarens namn, och
- ett undertecknande med stöd av e-legitimation innebär att användaren vill att den elektroniska underskriften ska få samma verkan som om användaren hade skrivit under på papper samt att användaren, innan underskrift sker, noga måste granska det som presenteras för underskrift och ta ställning till om han eller hon vill skriva under.

Varje beskrivning behöver samordnas med övrig juridisk och teknisk information samt presenteras med användargränssnitt som gör det lätt att finna information om de tjänster som myndigheten tillhandahåller.

6.3 Bindande användarvillkor för angivna tjänster

Vid inloggning i eget utrymme bör användaren med en aktiv handling få acceptera vissa användarvillkor för att ges tillträde. Det bör av dessa villkor följa vad som gäller för utrymmet, vem tillhandahållaren är och för vilken eller vilka presentations- eller servicetjänster utrymmet används.

Beskrivningen av eget utrymme behöver presenteras tydligt med användargränssnitt som leder till bindande användarvillkor, när regler införs genom avtal. Regleras utrymmet i stället genom myndighetsföreskrifter blir de bindande efter att ha kungjorts i en författningssamling.[36] Användarvillkoren får inte stå i strid med vad som följer av en myndighetsföreskrift eller någon annan bestämmelse i författning.

Det bör införas ett fält i samband med inloggning i eget utrymme så att användaren, för att tillträde ska ges, tydligt får markera om han eller hon accepterar användarvillkoren (s.k. klickavtal).[37] I villkoren tas de regler in som behövs för att utrymmet ska hanteras rätt samt vad som blir följden om utrymmet missbrukas. Där bör också tydligt framgå vilka som ingår avtalet, dvs. vilka parterna är, och för vilken eller vilka service- eller presentationstjänster som utrymmet brukas.

Det egna utrymmet finns i anknytning till den service- eller presentationstjänst som utrymmet ska stödja. Användarvillkoren kan därför också behöva innehålla villkor för service- respektive presentationstjänsten. I så fall kan villkoren för utrymmet och de villkor som därutöver ska gälla för e-tjänsten införas genom klickavtal där de samlade villkoren ingår. Sådana tjänster kan också kräva att avtal sluts på förhand, t.ex. för att behöriga firmatecknare behöver tilldela behörighet åt berörda användare.

Klickavtal kan ingås så att en användare, som identifieras på ett säkert sätt, i samband därmed klickar i en ruta om att villkoren accepteras eller liknande uttryck. För avtal av särskild betydelse eller där risken för missbruk är mera påtaglig kan även underskrift införas, elektroniskt eller på papper. Men i så fall behövs också ett uppdaterat register knutet till berörd service- eller presentationstjänst där det framgår vilka användare som ska ha tillträde till följd av ett redan slutet avtal och där behörigheter som inte längre ska gälla blir avregistrerade utan dröjsmål. Här aktualiseras bl.a. elektronisk hantering av fullmakter och kontroller med hjälp av uppgifter i offentliga register där det med rättsverkan publiceras vilka personer som är behöriga att företräda en juridisk person. Frågor om elektronisk behörighetshantering är dock av en sådan omfattning att de inte kan behandlas här.

---

[36] Regler kan av närmast praktiska skäl sällan ges i lag eller förordning med den detaljeringsgrad som behövs för eget utrymme.

[37] Hanteringen av klickavtal bör utformas så att användaren med stöd av webbkakor, s.k. cookies, eller liknande inte behöver acceptera villkor för varje inloggning.

6.3.1 Regler för användare

Hur ett eget utrymme får användas beror på vilka ändamål det tillhandahålls för och vilka servicefunktioner som finns där. Preciserade användarvillkor bör införas.

En central del i användarvillkor för eget utrymme är hur utrymmet får brukas och därmed vad som ska vara förbjudet att göra med utrymmet. Som framgått är denna fråga också beroende av vilka funktioner som tillhandahålls i utrymmet. Vägledningen utgår här från ett eget utrymme som innehåller alla de funktioner som har berörts i avsnitt 6.2.3.

Användarvillkoren bör *inledningsvis* ange att utrymmet bara får användas för ändamål som är förenliga med den service- eller presentationstjänst som utrymmet ska stödja och endast i enlighet med tillämpliga regler och de tekniska och administrativa begränsningar som myndigheten har infört. Vanligtvis är eget utrymme knutet till en viss service- eller presentationstjänst, men någon absolut sådan begränsning finns inte. Är en bredare användning avsedd bör detta tydligt framgå för användaren, inte bara av den beskrivning som avses i avsnitt 6.2.2 utan även av villkoren för utrymmet.

En sådan bestämmelse, som anger den yttre ramen för tillåten användning av utrymmet, bör kompletteras med tydliga användarvillkor för att missbruk av eget utrymme inte ska uppkomma. Ändamålet för aktuellt utrymme blir här av särskild betydelse. Villkor kan behövas om att användaren inte får föra in eller bevara uppgifter eller handlingar som saknar betydelse för det ändamål som har bestämts för utrymmet och att sådana uppgifter eller handlingar genast ska rensas bort. Villkor kan vidare behövas enligt vilka en uppgift eller en handling genast ska tas bort om den behandlas i strid mot reglerna om persondataskydd, innehåller säkerhetsmässigt skadlig information, t.ex. skadlig kod, eller hanteras genom brottslig underlåtenhet eller handling.

Utöver detta kan kompletterande, mera preciserade villkor, visa sig nödvändiga. Det kan exempelvis vara fråga om regler enligt vilka användaren inte får bruka utrymmet

- i andra syften än dem som utrymmet tillhandahålls för, t.ex. inte som en alternativ kanal för kommunikation eller för annan lagring eller spridning av uppgifter, och inte heller annars så att det inverkar negativt på förtroendet för Myndighetens elektroniska tjänster, eller
- så att det kan uppkomma brister i skyddet för informationssäkerheten; bl.a. att användaren inte får nyttja utrymmet i strid med E-legitimationsnämndens regelverk för Svensk e-legitimation eller de villkor som gäller för användningen av e-legitimation i förhållande till utfärdaren av den.

Det kan vidare, när särskilda risker är förenade med en viss typ av eget utrymme, behövas regler om att en användare som upptäcker att någon missbrukar eller har missbrukat utrymmet ska rapportera detta till myndigheten utan dröjsmål.

När det inte finns någon offentligrättslig reglering av berört område bör regler införas genom användarvillkor för att motverka att användare missbrukar eget utrymme (angående reglering genom avtal, se avsnitt 5.7).

För utrymmen som används under längre tid kan det också behövas regler om hur tillgång får ges till uppgifter om innehavaren dör eller t.ex. går i konkurs.

6.3.2 Verkan av missbruk

En myndighet som tillhandahåller eget utrymme bör få ta bort ett utrymme om det är sannolikt att utrymmet missbrukats. Även andra åtgärder bör få vidtas om de är proportionella i förhållande till missbruket. Användaren bör underrättas om dennes utrymme har missbrukats.

För att hindra missbruk av eget utrymme eller i vart fall motverka att skyddet för information i utrymmet bryts igenom, till följd av åtgärder som tillhandahållaren måste vidta vid missbruk av ett utrymme, bör tydliga regler införas om vad myndigheten får göra. Eget utrymme har i många fall en sådan utformning att användaren utan orimliga insatser kan börja om från början. Tillhandahållande myndighet bör därför vanligtvis få ta bort ett utrymme om det är sannolikt att det har missbrukats. Åtgärden bör emellertid vidtas endast om den är proportionell i förhållande till dels missbrukets art, dels det men som kan antas uppkomma för utrymmesinnehavaren. En myndighet bör redan när ett eget utrymme utformas och införs överväga vilka åtgärder som kan vara lämpliga och proportionella samt vilka alternativa förfaranden som kan komma ifråga när ett missbruk har upptäckts. Det är emellertid svårt att här närmare ange hur åtgärderna bör vara utformade.

En allmänt hållen regel om åtgärder vid missbruk kan därför vara lämplig, kombinerad med en regel om att ett ingrepp av myndigheten måste vara proportionellt. En regel bör samtidigt införas om att tillhandahållande myndighet helt får hindra tillhandahållande till användare som har agerat särskilt hänsynslöst. En åtgärd med anledning av ett missbruk bör dock inte få fortgå längre än vad som är försvarligt med hänsyn till omständigheterna.

Skulle någon annan än användaren missbruka en användares utrymme bör tillhandahållande myndighet vara skyldig att utan onödigt dröjsmål underrätta användaren om detta.

6.4 Regler för myndigheter

Hur en myndighet får förfara med ett eget utrymme beror på de ändamål för vilka det tillhandahålls och de servicefunktioner som ska finnas där. Preciserade regler bör kombineras med tekniska begränsningar så att eget utrymme skyddas från insyn av myndighetens personal eller annan. I avtal kan hänvisas till gällande arbetsordningar och instruktioner för eget utrymme.

Det är inte bara användaren som ska följa regler så att utrymmet brukas rätt. Myndigheten ska utforma och tillhandahålla eget utrymme så att det får den juridiska status och de tekniska och administrativa egenskaper som användaren med fog förväntar sig (se kap. 4). Utrymmet ska därför konstrueras så

att det uppfyller rekvisiten i vissa rättsregler och så att ingen annan än användaren bereder sig tillgång till innehållet i utrymmet eller annars förfogar över det. Myndigheten behöver utforma utrymmets servicefunktioner och den tillhörande drift- och säkerhetsrelaterade hanteringen så att den inte ger plats för missbruk. Tekniska och administrativa begränsningar behöver knytas till de ändamål för vilka myndigheten tillhandahåller utrymmet så att det inte kan brukas av användare för annat än vad tillhandahållaren avser. Exempelvis bör fritextfält så långt möjligt begränsas genom användning av formulär och fasta svarsalternativ och när de tillåts kombineras med tekniska begränsningar av möjligheterna att lägga in kod i fälten.

Detta skydd behöver kompletteras med regler som ger en tydlig ram för myndighetens åtgärder och skyldigheter när den tillhandahåller eget utrymme. Sådana regler kan behöva innefatta att myndigheten ska behandla handlingar, inställningar och andra uppgifter i användares eget utrymme endast som led i teknisk bearbetning eller teknisk lagring för användarens räkning, hålla information i eget utrymme avskild från myndighetens verksamhetssystem och skydda de uppgifter och handlingar som finns i eget utrymme så att ingen annan än användaren tar del av innehållet och att informationen i övrigt ges ett adekvat skydd. Att myndigheten ska vidta de tekniska och organisatoriska åtgärder som behövs för att åstadkomma den säkerhetsnivå som enligt författning krävs från bl.a. integritets- och informationssäkerhetssynpunkt är en viktig del. Dessa skyldigheter kan emellertid redan framgå av föreskrifter, arbetsordningar eller instruktioner om informationssäkerhet inom myndigheten. Även här kan närmare regler behövas, beroende på ändamålet med det aktuella utrymmet och vilka servicefunktioner som myndigheten inför där.

Regler för myndigheten och dess personal kan därför även behöva innefatta att särskilt skydda uppgifter i eget utrymme, så att användares bruk av eget utrymme inte kartläggs eller övervakas och att myndighetens personal och utomstående inte får insyn i uppgifter eller handlingar i utrymmet (utlämnande enligt 2 kap. TF eller 6 kap. 4-5 §§ OSL kommer inte i fråga). Där bör också anges att befattningshavare som för myndighetens räkning sköter eget utrymme inte får ha någon arbetsuppgift som är inriktad på informationsinnehåll i eget utrymme.

Här behöver också vissa nödliknande situationer uppmärksammas. I speciella undantagsfall kan ett tekniskt fel eller en brist som visar sig finnas i informationssäkerheten göra det nödvändigt för någon med särskild behörighet att vidta reparations- eller skyddsåtgärder, med en sådan särskild behörighet att det inte med fullständig visshet kan uteslutas att den som utför åtgärden inte kan råka få se en uppgift i ett utrymme. Myndigheten bör därför införa tydliga regler enligt vilka endast någon eller några enstaka särskilt betrodda personer får ha sådan teknisk tillgång till systemet att uppgifter i eget utrymme kan bli tillgängliga i läsbar eller annars uppfattar form. Dessa befattningshavare behöver samtidigt förbjudas att använda sin åtkomst i annat fall än när det är nödvändigt för att rätta fel eller vidta åtgärder som är nödvändiga från informationssäkerhetssynpunkt. De ska också instrueras att genast sluta läsa om en uppgift i ett eget utrymme trots allt skulle bli synlig och att vidta de åtgärder i övrigt som krävs för att uppgifterna inte ska bli tillgängliga för annan än användaren.

Eget utrymme bör dessutom utformas så att gränssnitt och funktioner hindrar eller i vart fall motverkar felaktiga, skadliga, olagliga eller annars olämpliga behandlingar av uppgifter. Vid misstanke om att ett utrymme använts för brott ska uppgifter i utrymmet inte lämnas ut utan stöd av ett straffprocessuellt tvångsmedel eller användarens samtycke.[38]

Regler behövs också om hur den myndighet som tillhandahåller eget utrymme får och ska agera när en viss användares utrymme inte längre behövs eller om en extraordinär brottslig händelse eller ett tekniskt missöde har resulterat i att uppgifter kommit att bli tillgängliga för någon annan. I denna del kan regler behöva införas om att myndigheten avslutar eget utrymme och rensar bort de uppgifter som finns där, när utrymmet inte längre behövs med hänsyn till ändamålet med det, alternativt att myndigheten tar bort utrymmet och de uppgifter som finns där när en användare inte har brukat sitt utrymme under en viss tid (som angetts i villkoren för användaren).

Är det i stället fråga om ett sådant utrymme som myndigheten tillhandahåller endast under den tid som en inloggning pågår, tar myndigheten bort de uppgifter som finns i utrymmet så snart användaren har loggat ut. När ett till tiden begränsat utrymme tillhandahålls ska myndigheten tydligt informera användaren om att tjänsten begränsats på detta sätt och att uppgifterna tas bort. Myndigheten ska ha en automatiserad rutin som innebär att uppgifterna därefter omedelbart rensas bort. Skulle en extraordinär händelse, såsom ett brottsligt angrepp eller ett teknisk missöde, leda till att innehållet i ett utrymme blir allmän handling bör det finnas ett redan fattat gallringsbeslut och rutiner för att omedelbart gallra uppgifterna, om de inte krävs för att utreda brott. Sådan gallring avser inte användares uppgifter i ett alltjämt skyddat utrymme utan uppgifter som felaktigt blivit allmän handling hos myndigheten.

Reglerna bör dessutom innefatta att myndigheten, om det uppkommer ett tekniskt eller administrativt fel som avser ett eget utrymme, ska avhjälpa felet med den skyndsamhet som omständigheterna kräver.

Myndigheten bör dessutom tillhandahålla en hjälptjänst åt användare av eget utrymme. Tjänsten får emellertid inte utformas så att Myndigheten får tillträde till användares eget utrymme. Krävs det att befattningshavare vid hjälptjänsten får ta del av sådana uppgifter måste användaren först lämna ut dem ur sitt utrymme till myndigheten. Användaren ska i så fall först ha informerats om följderna från offentlighetssynpunkt. Lämnar Användaren ut uppgifter till hjälptjänsten ska myndigheten vidta särskilda åtgärder för att skydda dessa uppgifter från insyn av utomstående, t.ex. genom en gallringsrutin som innebär att uppgift tas bort så snart hjälpen har lämnats.

Beskrivna handlingsregler för den myndighet som tillhandahåller eget utrymme tar i allt väsentligt sikte på hur de befattningshavare som sköter den tekniska utformningen och driften av eget utrymme ska förfara i sådana undantagsfall där en åtgärd kan beröra innehållet i ett eget utrymme eller när

[38] Detta hindrar inte att en polisanmälan görs när det finns en misstanke om brott.

ett eget utrymme behöver tas bort helt eller rensas från vissa uppgifter. En naturlig plats för sådana bestämmelser är de arbetsordningar och instruktioner som gäller för myndighetens hantering av eget utrymme, särskilt som eget utrymme tillhandahålls som en service utan någon ersättning från användaren. Det kan därför vara lämpligt att i användarvillkor för eget utrymme endast hänvisa till de regler som gäller internt för myndigheten.

Har myndigheten utkontrakterat driften av eget utrymme behöver motsvarande villkor införas i avtal med underleverantören så att utrymmesinnehavaren ges skydd mot obehörig insyn av underleverantörens personal.

6.5 Övriga frågor

Civilrättsliga avtal brukar innehålla ett antal övriga regler om olika mer eller mindre perifera frågor, bl.a. om immateriella rättigheter. I ett kortfattat klickavtal för eget utrymme bör regler av detta slag dock i huvudsak kunna undvaras. Det kan emellertid, eftersom hanteringen av eget utrymme är under snabb utveckling, vara lämpligt att i användarvillkor ta in regler om ändring av villkor och om hur meddelanden rörande avtalet lämnas elektroniskt.

Eftersom användningen av elektroniska tjänster sker närmast oberoende av landsgränser kan det vidare vara lämpligt att i avtal föra in att avtalet ska tolkas och tillämpas i enlighet med svensk rätt, att svenska lagvalsregler inte ska vara tillämpliga och att tvister angående tolkningen eller tillämpningen av användarvillkoren och därmed sammanhängande rättsförhållanden ska avgöras av svensk domstol.

***

eSamverkansprogrammet (eSam) är en frivillig fortsättning efter E-delegationen och består av 19 medlemmar. Syftet med programmet är att vara ett forum för fortsatt samverkan mellan myndigheter och SKL och ska bygga vidare på de kunskaper och erfarenheter som byggts upp inom ramen för E-delegationen. En viktig uppgift för programmet är att ge ut vägledningar som skapar förutsättningar för att öka den digitala samverkan inom offentlig förvaltning.

Arbetsförmedlingen, Bolagsverket, Centrala Studiestödsnämnden, eHälsomyndigheten, Ekonomistyrningsverket, Försäkringskassan, Jordbruksverket, Kronofogdemyndigheten, Lantmäteriet, Migrationsverket, Naturvårdsverket, Pensionsmyndigheten, Polisen, Riksarkivet, Skatteverket, Sveriges Kommuner och Landsting, Tillväxtverket, Transportstyrelsen och Tullverket (april 2016).

eSam