Juridisk vägledning för

verksamhetsutveckling inom e-förvaltning 3.0

eSam

Förord

Digitala verktyg och tjänster möjliggör nya former och sätt att erbjuda service och välfärdstjänster. Samtidigt bidrar de till en effektivare offentlig verksamhet. Verksamhetsutveckling inom offentlig sektor handlar därför alltmer om att använda digitaliseringens möjligheter för att möta den snabba utvecklingen i omvärlden (prop. 2016/17:198 s. 5). När sådana verktyg och tjänster utvecklas krävs rättsliga bedömningar för att kombinera teknik och juridik på ett rättsenligt och i övrigt lämpligt sätt.

En juridisk vägledning för verksamhetsutveckling inom e-förvaltningen utarbetades av E-delegationens rättsliga expertgrupp (version 1.0) och beslutades år 2013 av E-delegationen[1]. I vägledningen gjordes bedömningar och tolkningar av rättsläget som ett stort antal myndigheter och organisationer står bakom och som har lagts till grund för utformningen av e-tjänster. År 2015 gavs denna vägledning ut i en ny omarbetad version (2.0).

E-delegationens juridiska bedömningar har numera fått visst stöd i rättspraxis och lagstiftningsärenden från senare tid. Redovisade funktioner och rättsliga bedömningar har således tillämpats under ett antal år och stärkts genom den rättsutveckling som ägt rum inom området. Myndigheterna bör ta tillvara dessa klargöranden i sitt fortsatta arbete med att införa e-tjänster. Därför har eSamverkansprogrammets[2] (eSams) rättsliga expertgrupp utarbetat en uppdaterad juridisk vägledning. Inom ramen för detta arbete har även den ökande användningen av bastjänster belysts liksom möjligheterna att fatta beslut helt automatiserat och att ersätta direktåtkomst med utlämnande i annan form.

[1] E-delegationen var en kommitté under Finansdepartementet vars uppdrag avslutades år 2015. Delegationen hade i uppdrag att driva på e-förvaltningsutvecklingen i offentlig sektor. Sveriges Kommuner och Landsting (SKL) och 16 statliga myndigheter ingick i delegationen. Dir 2009:19 http://www.regeringen.se/rattsdokument/kommittedirektiv/2009/04/dir.-200919/

[2] eSam är en frivillig fortsättning efter E-delegationen och består idag av 24 statliga myndigheter och Sveriges Kommuner och Landsting (SKL). Se mer www.esamverka.se

Innehåll

1. Inledning

eSam vill med denna vägledning stödja digitaliseringen av offentlig sektor, dels genom att den kan utgöra en grund för en myndighets policydokument men även som stöd i en myndighets bedömning i ett enskilt fall, det vill säga när myndigheten överväger att införa en viss digital tjänst.

1.1 Syfte med denna vägledning

E-tjänster kan utformas på många olika sätt. Det är den enskilda myndigheten som bestämmer hur dess e-tjänster ska vara utformade och hur tjänsterna ska få användas (prop. 2016/17:198 s. 6). Denna vägledning förklarar juridiska frågor som är centrala vid utvecklingen av sådana tjänster och presenterar rättsliga bedömningar för att kombinera teknik och juridik på ett rättsenligt och i övrigt lämpligt sätt.

Flera av de funktioner som beskrivs utgör etablerad myndighetspraxis och har fått en omfattande tillämpning. Exempelvis sjösattes elektronisk skattedeklaration med s.k. eget utrymme redan år 2001. Sådana servicetjänster tillhandahålls numera av i stort sett varje myndighet som erbjuder it-baserade tjänster.

Genom att återanvända de funktioner som beskrivs i vägledningen kan myndigheter uppnå förenklingar och tidsbesparingar vid verksamhetsutveckling. Ett syfte är samtidigt att myndigheter ska kunna begränsa sina rättsliga risker genom att ta tillvara de juridiska bedömningar som gjorts i samverkan inom E-delegationen och vidareutvecklats inom eSam.

Genom att återanvända de funktioner som beskrivs i vägledningen kan myndigheter uppnå förenklingar och tidsbesparingar vid verksamhetsutveckling.

1.2 Målgrupp

Denna vägledning ska kunna fungera som en bro mellan teknik och juridik. För att ta fram it-baserade lösningar som är juridiskt korrekta krävs samarbete, inte bara mellan verksamhetsutvecklare, säkerhetsansvariga, arkitekter, arkivarier och jurister utan även med alla som på något sätt är involverade i att ta fram en lösning (till exempel beställare, chefer, controllers, kommunikatörer och projektledare). Alla dessa yrkeskategorier är därför målgrupp för denna vägledning. Vägledningen är dessutom av betydelse för externa leverantörer som behöver anpassa sina tjänster till e-förvaltningens behov.

Genom att vara väl insatt i de tekniska och juridiska förutsättningarna blir det enklare för dem att i samverkan ta fram nya it-baserade tjänster och förbättra de tjänster som redan har utvecklats.

Denna vägledning ska kunna fungera som en bro mellan teknik och juridik.

1.3 Läsanvisning och nyheter

Detta är den tredje versionen av vägledningen. De två första har beslutats av E-delegationen medan denna beslutats av eSam.

I denna version har använda begrepp uppdaterats. Bland annat har definitioner införts av egen hämtning och egen delning (avsnitt 2.1). Vägledningen har kompletterats genom att regler och metoder berörts för automatiserade beslut (avsnitt 2.8) och för utlämnande av uppgifter utan att direktåtkomst uppkommer (avsnitt 2.7). Redovisningen har renodlats bland annat genom att beskrivningar av bastjänster arbetats in i kapitlen om servicetjänster (kap. 6) och presentationstjänster (kap. 7). Den har vidare fördjupats genom en redovisning av krav på eget utrymme (avsnitt 2.6) och av de numera aktuella frågorna om

användare eller företag ska tilldelas eget utrymme samt om ett eller flera egna utrymmen ska tilldelas för den service som ges med stöd av sådana funktioner (se avsnitt 6.1.1, 6.4, 7.2). Vidareförmedlingstjänster har också berörts (avsnitt 6.5) och nya möjligheter att informera med stöd av indexinformation (avsnitt 7.1.1).

Dessutom har rättsläget i vissa delar blivit tydligare till följd av ny rättspraxis och ny lagstiftning med tillhörande motivuttalanden. Dessa nyheter har kortfattat redovisats i avsnitt 2.2.[3]

De juridiska lösningar som redovisas kan användas som byggklossar som sätts samman på varierande sätt, anpassade till de juridiska och tekniska förutsättningar som gäller för den enskilda tillämpningen. Vid detta utvecklingsarbete ska myndigheterna sträva efter att lämna ut uppgifter på annat sätt än genom direktåtkomst, underlätta för användare genom att införa bastjänster, öka servicen och ta tillvara rationaliseringspotentialen genom automatiserade beslut.

Redovisningen bygger i huvudsak på it-arkitekturer och juridiska bedömningar som myndigheter har brukat under ett antal år, i vissa fall ända från 2000-talets inledande skede. Med it-arkitekturer brukar avses tekniska beskrivningar, som kan ha olika detaljeringsnivåer. Här beskrivs övergripande (del-)strukturer och hur de kan inordnas under gällande rätt.

Rättsläget vid en användning av dessa it-arkitekturer är inte heller nu helt klart. Vissa risker kan finnas om t.ex. en domstolsprövning skulle utfalla i en oväntad riktning. Härvid bör betonas att den behandling av uppgifter som äger rum på myndighetsområdet ska vara präglad av öppenhet, transparens och en god offentlighetsstruktur, oberoende av om elektroniska eller pappersbaserade rutiner används. Samtidigt är det en självklarhet att intressen av skydd för bl.a. enskildas hem, korrespondens och integritet i övrigt måste värnas.

För ytterligare juridiskt stöd hänvisas till kommentaren i kap. 9.

1.4 Medverkande

Arbetet med att ta fram vägledningen har genomförts av eSams rättsliga expertgrupp. Ledamöter i expertgruppen är Johan Bålman, Eva Maria Broberg, Malgorzata Drewniak, Per Furberg, Linn Kempe, Gustaf Johnssén, Jan Sjösten, Gunnar Svensson, Mikael Westberg, Staffan Wikell, Tomas Öhrn och Christina Wikström. Adjungerade ledamöter i expertgruppen är Maria Sertcanli, och Veronica Eckerby. I arbetet har även eSams rättsliga referensgrupp och expertgrupperna för säkerhet och arkitektur deltagit.

[3] Jfr bland annat eSams promemoria den 22 november 2017 Eget utrymme är numera accepterat i lagmotiv – men vilka juridiska krav ställs på eget utrymme? (www.esamverka.se/stod-och-vagledning/rattsliga-uttalanden/eget-utrymme.html).

2. Utgångspunkter

2.1 Definitioner

I denna vägledning menas med:

Tjänster	
E-tjänst (även kallad digital[4] tjänst)	En it-baserad tjänst som har ett användargränssnitt för kommunikation mellan människa och maskin.
Bastjänst (även kallad applikations-programmeringsgränssnitt, API)	En it-baserad tjänst som har ett applikationsgränssnitt för kommunikation från maskin till maskin.
Vidareförmedlingstjänst (även kallad sammansatt bastjänst)	Bastjänster som är sammansatta så att uppgifter hämtas från flera källor.
Servicetjänst	En e-tjänst där en innehavare av ett eget utrymme kan utforma utkast till handlingar i sitt utrymme, få uppgifter förifyllda eller annars utlämnade, antingen av den som tillhandahåller utrymmet eller annan med stöd av egen hämtning eller egen delning, sända handlingar till en mottagnings-funktion och vidta andra nödvändiga åtgärder.
Presentationstjänst	En e-tjänst där innehavaren av ett eget utrymme får handlingar visade utan att det som visas ska bli tillgängligt för andra.
Hjälptjänst	En tjänst för att ge hjälp till en användare eller att förklara uppgifter som lämnas till användaren där information som skriftligen inkommer till myndigheten blir allmän handling.

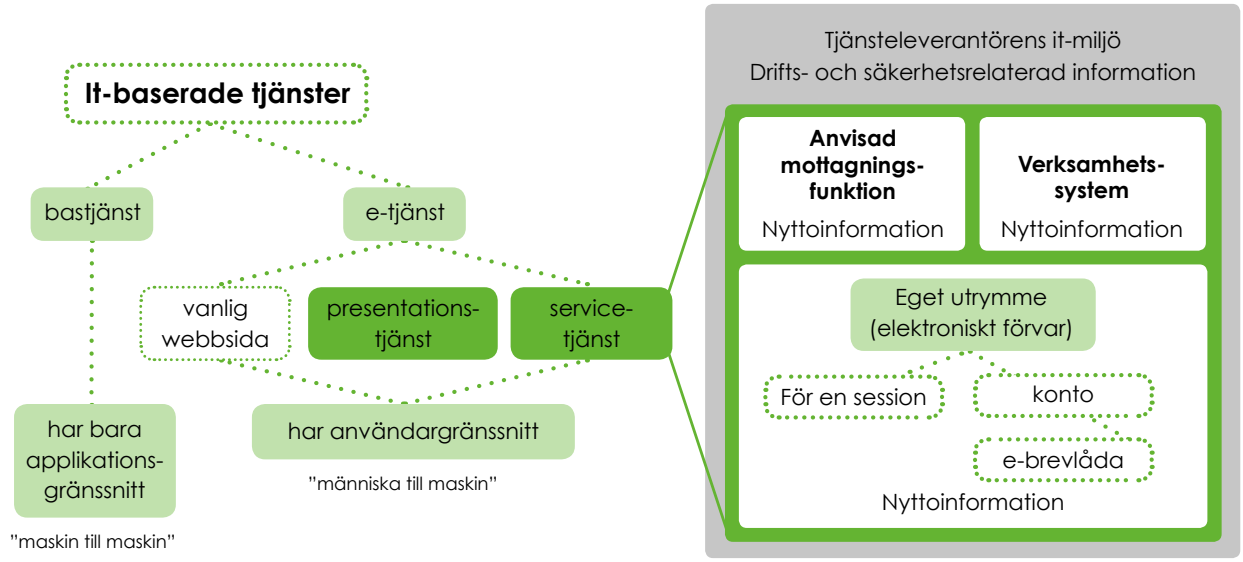
Enskildas skyddade utrymmen och skyddade hantering	
Eget utrymme	Ett skyddat förvar som tillhandahålls enligt 2 kap. 10 § första stycket TF endast som led i teknisk bearbetning eller teknisk lagring för annans räkning.
Egen hämtning	När en innehavare av ett eget utrymme från utrymmet begär uppgifter och får dem utlämnade direkt till sitt eget utrymme.
Egen delning	När en innehavare av ett eget utrymme genom en aktiv åtgärd eller automatiserat överför uppgifter från utrymmet till ett annat utrymme.
Serviceskede	Ett skyddat förlopp där en användare hanterar uppgifter så att a) service ges enligt förvaltningslagen (2017:900; FL), b) ingen utomstående avses ha insyn i de uppgifter som behandlas, och c) det inte sker någon ärendehandläggning.

Tjänstelevererande myndighets it-miljö	
Mottagningsfunktion	En funktion där en myndighet som tillhandahåller en it-baserad tjänst mottar handlingar, ankomstregistrerar dem och i många fall även sänder kvittens.
Verksamhetssystem	Den it-miljö där en myndighet utför sitt arbete
Nyttoinformation	Uppgifter som är till för enskilda eller befattningshavare, t.ex. ett utkast i ett eget utrymme eller en inkommen ansökan, till skillnad från drift- och säkerhetsrelaterad information.[5]
Drifts- och säkerhetsrelaterad information	Data som krävs för en effektiv och säker drift av informationssystem.[6]

[4] Jfr däremot NIS-direktivet och den författningsreglering som föreslagits där ”digital tjänst” getts en mera begränsad innebörd.
[5] Angående detta uttryck, se prop. 2016/17:198 s. 14.
[6] Angående detta uttryck, se avsnitt 4.1.4 (särskilt not 40).

Sambanden mellan dessa begrepp och vissa anknytande termer framgår av följande figur där det också delvis visas hur de kan brukas.

Figur 1, Använda begrepp



Till detta kommer vissa begrepp som redovisas i avsnitt 4.1 som rättsfigurer. Dessa begrepp och definitioner speglar utvecklingen på det stadium där denna vägledning antogs och bör därför inte tolkas eller tillämpas så att innovationer och förbättringar motverkas.

2.2 Ett förtydligat rättsläge

De bedömningar som redovisas i vissa rättskällor kan ge stöd för juridiskt hållbara it-baserade tjänster.

Verksamhetsutveckling på myndighetsområdet har etablerat it-arkitekturer och processer för de tekniska och administrativa led som en användare går igenom i en it-baserad tjänst. Motsvarande anpassningar av de rättsliga synsätten har bara delvis ägt rum.

I denna vägledning tar eSam tillvara ny författningsreglering och rättspraxis som rör it-baserade tjänster samt de motivuttalanden som tillkommit på området, bl.a.

1. Regeringens proposition 2016/17:180 En modern och rättssäker förvaltning – ny förvaltningslag, där ny reglering lagts fram för bl.a. inkommande handlingar och uttalanden gjorts som ger stöd för e-tjänster,
2. Regeringens proposition 2016/17:198 Utökat sekretesskydd i verksamhet för teknisk bearbetning och lagring, där sekretessen – och därmed tystnadsplikten – utvidgats för eget utrymme och uttalanden gjorts, om bl.a. eget utrymme, som blir av central betydelse för den juridiska bedömningen av e-tjänster,

3. Regeringens proposition 2012/13:74 Förfalsknings- och sanningsbrotten, genom vilken bl.a. förfalskning i it-miljö, förnekande av e-underskrift och missbruk av e-legitimation har kriminaliserats,
4. Högsta förvaltningsdomstolens dom i det så kallade LEFI Online-målet (HFD 2015 ref. 61), där domstolen funnit att direktåtkomst och s.k. överskottsinformation avgränsas genom en prövning av om berörd handling anses vara förvarad enligt 2 kap. 3 § andra stycket TF hos mottagande myndighet,
5. Högsta domstolens dom den 22 december 2017 i mål nr T 435-17, där domstolen uttalat sig rörande vissa bevisfrågor vid användningen av e-underskrifter, och
6. underrättspraxis där eget utrymme har ansetts vara utformat så att de handlingar som finns i utrymmet, enligt 2 kap. 10 § tryckfrihetsförordningen (TF), är undantagna från offentlighetsinsyn.[7]

De bedömningar som redovisas i dessa rättskällor ger stöd för it-baserade tjänster, anpassade till reglerna om offentlighet och sekretess, inkommande och service och fördelning av juridiskt ansvar.

2.3 Vägledningen utgår från service- och presentationstjänster

Eftersom servicetjänster och presentationstjänster utgör grunden för den snabbt framväxande e-förvaltningen tar vägledningen sin utgångspunkt i dem.

Myndigheter har sedan länge tillhandahållit webbsidor där var och en kan ta del av information. I och med införandet av e-legitimationer har det också blivit möjligt att legitimera sig och skriva under via internet.[8] Myndigheter har härigenom fått nya möjligheter att tillhandahålla servicetjänster där användare kan utforma, skriva under och ge in handlingar och presentationstjänster där användare kan ta del av samlad information på ett enkelt sätt. Avsikten är att förenkla för medborgare och företag utan att rättssäkerheten försämras jämfört med traditionell pappersmiljö.[9] Detta har blivit möjligt genom bl.a. säker användaridentifiering.

Det interaktiva stöd som användaren ges i en servicetjänst har samtidigt fört med sig att utkasten inte längre upprättas hos användaren i dennes dator. De upprättas i stället i en elektronisk miljö som myndigheten tillhandahåller i

[7] Kammarrätten i Stockholm har i en dom den 26 oktober 2015 i mål nr 7369-15 bedömt att handlingar som förvarades i en CV-databas hos Arbetsförmedlingen, fick anses vara förvarade hos myndigheten endast som led i teknisk bearbetning eller teknisk lagring för annans räkning. CV-databasen bestod av konton för arbetssökande och arbetsgivare. De arbetssökande kunde lagra CV och annan information i ett eget utrymme och arbetsgivare söka bland profilerna, läsa dem och skicka förfrågningar.

[8] Se vidare eSams publikation Juridisk vägledning för införande av e-legitimering och e-underskrifter.

[9] Författningsändringar har genomförts för att formföreskrifter inte ska hindra elektroniska rutiner, t.ex. på skatteområdet och området för företagsregistrering, så att elektroniska underskrifter likställts med underskrifter på papper. Frågan om inkommande handlingar har också genomlysts och en myndighetspraxis har vuxit fram för mottagningsfunktion; se bl.a. E-nämndens vägledning för hantering av inkommande elektroniska handlingar (e-nämnden 05:02), Per Furberg i Svensk Juristtidning, Inkommande handlingar – en IT-anpassad tolkning (SvJT 2005, s. 273 ff.) och Förvaltningslagsutredningens betänkande (SOU 2010:29) En ny förvaltningslag, s. 40 och s. 377 ff. Regeringen har emellertid avstått från att i en ny förvaltningslag införa en särskild regel för anvisad mottagningsfunktion, se prop. 2016/127:180. eSam har redovisat detta i ett rättsligt uttalande den 26 oktober 2017 Ankomstdag för elektroniska handlingar, med tillhörande promemoria den 31 oktober 2017 om inkommandetidpunkt.

anknytning till en e-tjänst, i ett eget utrymme där nyttoinformation finns som bara innehavaren av utrymmet ska få ta del av.[10] På liknande sätt behöver den som använder en presentationstjänst inte begära och få uppgifter översända från en eller flera myndigheter, så att användaren själv måste ställa samman uppgifterna. Istället hämtas informationen in av den som tillhandahåller presentationstjänsten och sammanställs automatiserat så att användaren kan ta del av sammanställt material i eget utrymme.

Information i ett sådant utrymme anses enligt en sedan länge etablerad myndighetspraxis inte vara inkommen till myndigheten enligt förvaltningslagen. Den används av innehavaren i ett serviceskede där ingen utomstående avses ha insyn i de uppgifter som behandlas. Dessa tjänster finns numera i flera varianter; i vissa fall med, i andra fall utan legitimering för tillträde, ibland med, ibland utan underskrift av handlingar som ges in. För att ett eget utrymme ska tillhandahållas krävs emellertid normalt att en användare först har legitimerat sig på ett säkert sätt.

Eftersom servicetjänster och presentationstjänster utgör grunden för den framväxande elektroniska förvaltningen tar denna vägledning sin utgångspunkt i dem, men vissa anknytande it-baserade tjänster tas också upp; bl.a. bastjänster och hjälptjänster.

Gränsen mellan presentationstjänster och servicetjänster kan visserligen vara delvis flytande men denna indelning fyller en funktion genom att presentationstjänsten knyter an till det som brukar kallas Mina sidor, där information samlas in och visas för en användare så att denne kan navigera rätt. Servicetjänsten förser istället typiskt sett en innehavare med en förifylld blankett som kompletteras av användaren, granskas, skrivs under och skickas till myndighetens mottagningsfunktion. Juridiska beskrivningar och bedömningar kan vanligtvis underlättas genom en sortering i dessa kategorier.

I servicetjänsten behöver innehavaren ha sin information ostört och utan insyn, på samma sätt som om denne befunnit sig i sin bostad eller på sitt tjänsterum. I en presentationstjänst kan mera omfattande information samlas in jämfört med traditionell miljö för att tillgodose den registrerades behov. Detta får inte leda till kartläggning eller övervakning.[11]

I servicetjänsten behöver innehavaren ha sin information ostört och utan insyn, på samma sätt som om denne befunnit sig i sin bostad eller på sitt tjänsterum.

2.4 Bastjänst även kallad API

Automatiserad hantering via bastjänster har blivit en allt viktigare del i utvecklingen av e-förvaltningen.

Som framgått av definitionerna i avsnitt 2.1 brukas en bastjänst (eller med en synonym ett applikationsprogrammeringsgränssnitt, API) för helt automatiserade procedurer maskin till maskin. Exempelvis kan en användare, istället för att logga in på en aktörs webbplats och med några klick fråga efter viss information och få den visad på sin skärm, använda en bastjänst som helt automatiserat skapar och överför denna begäran. Svar ges så att uppgifter utan manuella moment kan fogas in i sitt rätta sammanhang, t.ex. i en blankett som delvis blir förifylld i eget utrymme (se avsnitt 6.2). Vanligtvis sätts flera bastjänster samman så att information kan flöda mellan flera myndigheter helt automatiserat.

[10] Jfr hur det föreskrivs straffansvar för intrång i förvar, om någon utan lov bereder sig tillgång till annans brev eller tillslutna förvar (4 kap. 9 § BrB), och för dataintrång om någon olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling (4 kap. 9 c § BrB).

[11] Jämför 2 kap. 6 § andra stycket regeringsformen. Exempel på presentationstjänster inom ramen för E-delegationens och numera eSams arbete är Mina fullmakter och Min ärendeöversikt (prop. 2016/17:198 s. 9).

Som exempel på detta framgångsrika arbete kan nämnas Vidareförmedlingstjänsten för ekonomiska uppgifter (SSBTEK) och Vidareförmedlingstjänsten för grundläggande uppgifter om företag (SSBTGU).[12] Myndigheter inom eSam har härigenom utvecklat funktioner för att med sammansatta bastjänster hämta uppgifter från flera källor och att återanvända informationen, antingen så att det blir enklare för enskilda att ge in uppgifter på nytt (de förifylls) eller så att myndigheten hämtar uppgifter direkt till sitt verksamhetssystem utan att kräva att en enskild ska lämna uppgifterna på nytt.

Vägledningen innehöll tidigare ett särskilt kapitel om bastjänster. De används emellertid som en del i en servicetjänst, en presentationstjänst eller en hjälptjänst och har därför i denna vägledning inordnats under dessa tjänster, se avsnitt 6.5 och avsnitt 7.3 där det framgår att bastjänster kommit att bli en allt viktigare del i myndigheternas utveckling av e-förvaltningen.

2.5 Eget utrymme och nyttoinformation

Vägledningen utgår från tolkningar av gällande rätt som myndigheter sedan länge tillämpat vid sin utformning av it-baserade tjänster. Dessa tolkningar har nu fått stöd i motivuttalanden och rättspraxis så att skyddade elektroniska platser i form av eget utrymme kan tillhandahållas ”på nätet”.

Denna vägledning bygger på tolkningar av gällande rätt som myndigheter sedan länge har tillämpat vid utformningen av it-baserade tjänster. Information i eget utrymme (nyttoinformation) anses inte vara allmän handling hos den myndighet som tillhandahåller utrymmet. Undantaget i 2 kap. 10 § första stycket TF kan på så sätt tillgodose privatpersoners och företags förväntningar om att uppgifter i eget utrymme är skyddade från insyn och utlämnande med stöd av offentlighetsprincipen.

Handlingar i eget utrymme anses inte heller vara inkomna i förvaltningslagens mening. Därmed kan fysiska och juridiska personer ha arbetsmaterial i en tjänst på nätet med bibehållet skydd för individens privatliv och företagens intressen av närmast ekonomiskt slag. När den som innehar ett eget utrymme har bestämt sig för att lämna in en handling, genom att på ett aktivt och medvetet sätt skicka den från utrymmet till myndighetens elektroniska mottagningsfunktion, blir handlingen inkommen när den nått fram till mottagningsfunktionen.

Därmed kan fysiska och juridiska personer ha arbetsmaterial i en tjänst på nätet med bibehållet skydd för individens privatliv och företagens intressen av närmast ekonomiskt slag.

Dessa bedömningar stöds numera av uttalanden i motiven till en ny förvaltningslag och lagmotiven till en reglering av ett utökat sekretesskydd i verksamhet för teknisk bearbetning och lagring. I motiven till den nya förvaltningslagen beskrivs hur enskilda fyller i webbformulär på en myndighets server och skickar färdiga handlingar. Där uttalas vidare att det är möjligt att se den lagring som föregår ingivandet som en form av teknisk lagring för den enskildes räkning där handlingen inte blir att anse som allmän innan den har ”skickats in” (prop. 2016/17:180 s. 141). Samma bedömning har gjorts i den nämnda domen från Kammarrätten i Stockholm (se not 7).[13]

I lagmotiv rörande utökat sekretesskydd har regeringen dessutom valt att använda begreppet eget utrymme (prop. 2016/17:198 s. 7). Regeringen har

[12] Se https://www.forsakringskassan.se/myndigheter/e-tjanster/ssbtek och

[13] Det är en annan sak att frågan om när en elektronisk handling som skickats elektroniskt till en myndighet ska anses inkommen delvis har fallit mellan stolarna i det nämnda lagstiftningsärendet, se vidare avsnitt 4.1.1.

därvid förklarat att det finns stöd i rättspraxis för att myndigheter tillhandahåller digitala tjänster som uppfyller kraven i 2 kap. 10 § första stycket TF (a.prop. s. 16).[14] Där framgår vidare att myndigheter inte bara kan tillhandahålla servicetjänster som omfattas av 2 kap. 10 § första stycket TF, där eget utrymme används för att upprätta och skicka in handlingar till en mottagningsfunktion. Där förklaras att även presentationstjänster kan utformas så att myndigheters hantering av uppgifter sker enligt 2 kap. 10 § första stycket TF i form av teknisk bearbetning eller lagring för annans räkning. Sammanställningar kan därmed presenteras utan att tillhandahållande myndighet får ta del av det som visas (a.prop. s. 26).

Ett och samma informationsinnehåll kan alltså finnas både i eget utrymme (utan att vara allmän handling där), och i myndighetens verksamhetssystem (som allmän handling), efter att ett exemplar av handlingen skickats[15] till myndighetens funktion för att ta emot inkommande elektroniska handlingar.[16] På samma sätt kan en handling som bevaras (i ett exemplar) i myndighetens verksamhetssystem lämnas ut till eget utrymme (ett annat exemplar). Dessa olika exemplar av en handling i eget utrymme och i verksamhetssystem, bedöms var för sig från offentlighets- och sekretessynpunkt.[17]

Bestämmelsen i 2 kap. 10 § första stycket TF kan därmed tillämpas i enlighet med E-delegationens och eSams tolkning, så att skyddade elektroniska platser tillhandahålls ”på nätet” åt innehavare som behandlar uppgifter där i stället för lokalt i sin dator eller på papper i exempelvis en bostad eller ett tjänsterum.

2.6 Krav på eget utrymme

> Avgörande för om ett eget utrymme föreligger är om nyttoinformationen blir allmän handling eller inte. Enligt eSams bedömning behöver dock följande krav vara uppfyllda när eget utrymme tillhandahålls.

Enligt regeringens uttalanden i lagmotiven om utökad sekretess finns det inte vägledande avgöranden som ger tydligt besked om vilka av de egna utrymmen som myndigheter tillhandahåller som uppfyller kraven i 2 kap. 10 § första stycket TF (prop. 2016/17:198 s. 10 f.). Därför har eSam i ett rättsligt uttalande den 22 november 2017, Eget utrymme hos myndighet (dnr VER 2017:40), anfört att det måste vara en prioriterad åtgärd för myndigheterna att närmare klargöra dessa förutsättningar och att ge vägledning på området.

Under arbetet med dessa frågor har eSam emellertid valt att utvidga sin genomgång så att även anknytande krav på eget utrymme tas upp. I det följande redovisas därför inte bara vad som krävs för att handlingar i ett eget utrymme inte ska bli allmänna. Där berörs också vad som behöver beaktas för att

- ett tillräckligt sekretesskydd ska finnas (enligt OSL),

[14] Regeringen fann vidare E-delegationens förslag mera ändamålsenligt än andra alternativ som framförts i remissvar över utredningsförslaget (a.prop. s 15 f. och s. 19).
[15] Eget utrymme är i vissa fall utformat så att ett exemplar finns kvar där även efter att det skickats.
[16] Det är en annan sak att handlingar i eget utrymme ofta rensas bort så snart de har färdigställts och skickats till myndigheten.
[17] Regeringen har inte funnit stöd i gällande rätt för den invändning som hade förts fram mot eget utrymme, att det skulle saknas rättslig grund för att isolera ett tekniskt delmoment under den tid en handling förvaras hos en myndighet och betrakta det separat. Information kan alltså, vid tillämpningen av 2 kap. 10 § första stycket TF, förvaras i olika exemplar som bedöms var för sig.

- hanteringen ska följa de förvaltningsrättsliga, dataskyddsrättsliga och straffrättsliga reglerna, och
- uppgifterna ska ges ett tillräckligt skydd från informationssäkerhetssynpunkt.

Krav för att handlingar inte ska bli allmänna (2 kap. 10 § första stycket TF):

1. En myndighet som tillhandahåller eget utrymme får inte ta del av den information som finns där eller annars använda eller förfoga över uppgifterna för egen räkning (HFD 2011 ref. 52).
2. Det ska därför finnas förbud i författning, interna instruktioner eller i annan lämplig form mot att myndigheten använder uppgifter i eget utrymme för egen räkning eller annars förfogar över dem.
3. För att säkerställa skyddet ska dessutom endast viss teknisk personal hos en myndighet som tillhandahåller eget utrymme ha sådan behörighet att de kan bereda sig tillgång till uppgifter i eget utrymme.
4. Skulle personal råka läsa eller annars få del av information i eget utrymme, t.ex. när fel i system rättas eller åtgärder för informationssäkerheten vidtas, ska de ha instruerats att sluta läsa innehållet och att inte lämna ut eller annars använda uppgifterna.

De rekvisit som avgör om eget utrymme föreligger är utformade så att en myndighet kan tillhandahålla eget utrymme åt såväl privatpersoner och företag som andra myndigheter.

Krav för att ett tillräckligt sekretesskydd ska finnas:

1. Myndigheter som tillhandahåller it-baserade tjänster bör se till att uppgifter i ett serviceskede behandlas i eget utrymme eller annars så att de omfattas av stark sekretess, när innehavaren har en befogad förväntan att uppgifterna hanteras så att de är skyddade mot insyn (jfr 40 kap. 5 § OSL).[18]
2. En myndighet som själv sköter eget utrymme ska så långt det är möjligt ge tillträde för drift bara åt anställda och personal som på grund av uppdrag eller på annan liknande grund deltar i myndighetens verksamhet och därför omfattas av samma tystnadsplikt som anställda (2 kap. 1 § OSL).
3. En myndighet som utkontrakterar drift av eget utrymme ska så långt det är möjligt utforma och reglera uppdraget så att det är osannolikt att driftleverantörens personal tar del av eller vidarebefordrar uppgifter i eget utrymme.
4. En myndighet som utkontrakterat driften av eget utrymme bör enligt kontraktet inte ha rätt att ta del av den nyttoinformation som finns i eget utrymme.
5. Användare bör normalt identifieras med stöd av en e-legitimation med tillitsnivå 3 eller högre.[19]
6. Tar användaren del av uppgifterna för en juridisk persons räkning bör användarens behörighet kontrolleras.

[18] I särskilda fall kan dock omedelbar gallring, när sådan får ske, ge ett tillräckligt skydd.
[19] Se beträffande denna hantering eSams publikation Juridisk vägledning för införande av e-legitimering och e-underskrifter.

Krav från förvaltnings-, straff- och persondataskyddsrättsliga utgångspunkter:

1. Funktionerna ska utformas så att handlingar i eget utrymme inte blir inkomna i förvaltningsrättslig mening förrän de har nått myndighetens mottagningsfunktion.[20]
2. Myndigheten ska så långt det är praktiskt möjligt inte ha teknisk tillgång till eget utrymme så att innehållet omfattas av en registrerads rätt att enligt reglerna om persondataskydd få information om vilka personuppgifter som behandlas om denne.[21]
3. Myndigheten ska genom föreskrifter eller avtal om eget utrymme förbjuda sin personal att läsa innehåll i eget utrymme.
4. Myndigheten ska ha rätt att omedelbart gallra nyttoinformation som oavsiktligt blivit allmän handling.
5. Funktionerna får inte utformas så att de leder till övervakning eller kartläggning av enskildas personliga förhållanden eller andra liknande intrång i enskilds personliga integritet (prop. 2016/17:198 s. 24).
6. Det behöver finnas tydlig information om att e-legitimationer inte får missbrukas för att bereda tillträde för annan än den person som anges i legitimationshandlingen.[22]
7. Identifiering och behörighetskontroll behöver utföras på ett säkert sätt.

Informationssäkerhet och spårbarhet:

1. Se kap. 5.
2. Genom regler för eget utrymme bör behov av rensning och liknande åtgärder beaktas så att eget utrymme inte kan missbrukas.

En myndighet beslutar således själv hur den ska utforma sina tjänster och kan välja om eget utrymme ska tillhandahållas, vilken omfattning ett utrymme i så fall ska ha och hur länge det ska få finnas kvar, se vidare avsnitt 6.4 och 7.2. Myndigheten behöver härvid utveckla och anpassa sina tjänster i enlighet med den rättspraxis som växer fram inom området (prop. 2016/17:198 s. 16).

En myndighet beslutar således själv hur den ska utforma sina tjänster och kan välja om eget utrymme ska tillhandahållas

2.7 Elektroniskt informationsutbyte

> Rättsläget har delvis klarlagts genom att det i rättspraxis prövats vad som menas med direktåtkomst. Denna tolkning har samordnats med när en handling anses vara tillgänglig för en myndighet enligt 2 kap. 3 § andra stycket TF. Myndigheter bör så långt det är möjligt utforma informationsutbyten så att direktåtkomst inte uppkommer. På samma sätt bör egen hämtning och egen delning inte ske genom direktåtkomst.

Myndigheter som tillhandahåller it-baserade tjänster begär i många fall uppgifter från andra myndigheter i syfte att lämna ut dem till enskildas egna utrymmen (se avsnitt 2.5, 6.5 och 7.3). Eget utrymme kan också ha utformats så att innehavaren själv, från sitt utrymme, begär uppgifter och får dem direkt till

[20] Bara de handlingar som skickats från utrymmet så att de kommit in till myndigheten anses som framgått vara förvarade och inkomna i tryckfrihetsförordningens mening. Se beträffande motsvarande frågor om inkommande enligt förvaltningslagen, eSams rättsliga uttalande den 26 oktober 2017 Ankomstdag för elektroniska handlingar.
[21] Se eSams publikation Eget utrymme hos myndighet – en vägledning.
[22] Se eSams rättsliga uttalande den 24 april 2017 Missbruk av e-legitimation.

utrymmet (egen hämtning) eller överför uppgifter från ett eget utrymme till ett annat (egen delning), se avsnitt 4.1.3. Utformas detta informationsutbyte så att det uppstår direktåtkomst för en myndighet blir dock alla handlingar som den myndigheten kan nå allmänna där, oavsett om berörd handling redan har överförts till myndighetens it-miljö eller om det bara finns en möjlighet för en myndighet att komma åt informationen (jfr 11 kap. 4 § OSL).

Hanteringen kompliceras ytterligare av att många registerförfattningar innehåller olika regler för direktåtkomst respektive utlämnande på medium för automatiserad behandling. Det kan förhålla sig så att ett elektroniskt utlämnande får ske under förutsättning att det inte blir fråga om direktåtkomst.

Av integritetsskäl bör e-tjänster och eget utrymme normalt utformas så att direktåtkomst inte uppkommer. På samma sätt bör myndigheter utforma sitt informationsutbyte så att direktåtkomst inte uppkommer när den rättsliga osäkerhet som rått kring vad som menas med direktåtkomst har undanröjts av Högsta förvaltningsdomstolen i det s.k. LEFI Online-målet (HFD 2015 ref. 61). Där fann Högsta förvaltningsdomstolen att vad som utgör direktåtkomst avgränsas genom en prövning av om berörd handling anses vara förvarad enligt 2 kap. 3 § andra stycket TF hos mottagande myndighet. Om utlämnande myndighet måste reagera på en begäran om en handling finns inte sådan tillgänglighet som avses i 2 kap. 3 § andra stycket TF, se följande figur och eSams publikation Elektroniskt informationsutbyte – en vägledning för utlämnande i elektronisk form.

Att en registerlag medger direktåtkomst för en viss typ av utlämnande hindrar normalt inte att ett utlämnande istället sker på medium för automatiserad behandling.[23] Skyddade elektroniska platser kan därmed tillhandahållas ”på nätet” åt de som använder e-tjänster i stället för att de ska behandla uppgifterna lokalt i sin dator eller på papper i exempelvis en bostad eller ett tjänsterum. Samtidigt kan gränser upprätthållas mellan myndigheter även i it-miljö.

Myndigheterna bör klargöra om de funktioner de nu har i sina system verkligen är att anse som direktåtkomst enligt gällande rätt och, när ett lagstiftningsärende aktualiseras inom området, verka för att regler om direktåtkomst utmönstras i författning när det är praktiskt möjligt och lämpligt av integritetsskäl. Ytterligare avvägningar rörande integritetsskyddet behöver emellertid göras om direktåtkomst till enstaka uppgifter skulle ersättas med ett utlämnande på medium för automatiserad behandling där många uppgifter lämnas ut – inte bara de som behövs i det enskilda fallet.

Av integritetsskäl bör e-tjänster och eget utrymme normalt utformas så att direktåtkomst inte uppkommer.

[23] Att det kan finnas undantag framgår av bl.a. 2, 7 och 10 §§ lagen (2000:224) om fastighetsregister där det föreskrivs att personnummer får visas via direktåtkomst men endast i undantagsfall lämnas ut på medium för automatiserad behandling.

2.8 Automatiserade beslut

Rättsläget har klarlagts genom att det i förvaltningslagen föreskrivs att beslut får fattas automatiserat.

Det som hittills beskrivits avser i huvudsak den hantering som äger rum i ett serviceskede, dvs. före det att en handling når den funktion där myndigheten mottar den och påbörjar sin handläggning av ett ärende. Även myndighetens ärendehandläggning måste emellertid utföras med rättssäkra och rationella rutiner. En fråga som här föranlett en omfattande särreglering är om beslut får fattas automatiserat.[24]

Enligt 28 § första stycket förvaltningslagen (2017:900) kan beslut fattas automatiserat. Bestämmelsen träder i kraft den 1 juli 2018. Den förvaltningsrättsliga osäkerhet som funnits rörande myndigheternas rätt att utan särskild tillåtande författningsreglering fatta beslut automatiserat undanröjs med denna reglering.

Enligt artikel 22.1 i dataskyddsförordningen ska den registrerade visserligen ha rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripet profilering, vilket har rättsliga följder för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne.[25] Undantag från rättigheten att inte bli föremål för automatiserat individuellt beslutsfattande gäller emellertid för beslut som tillåts enligt nationell rätt som den personuppgiftsansvarige omfattas av och som fastställer lämpliga åtgärder till skydd för den registrerades rättigheter, friheter och berättigade intressen.

Den nya förvaltningslagen innehåller bestämmelser om kommunikation och rätt att lämna uppgifter muntligen, rätt till omprövning och rätt till överklagande. Därutöver finns även generella krav på legalitet, objektivitet och proportionalitet. Enligt eSams bedömning får därmed de generellt tillämpliga bestämmelserna i den nya förvaltningslagen[26] anses innefatta sådana lämpliga skyddsåtgärder för den registrerade att automatiserade beslut får fattas när de faller inom ramen för förvaltningslagens tillämpningsområde och är överklagbara.[27]

[24] E-delegationen föreslog i betänkandet Automatiserade beslut – färre regler ger tydligare reglering (SOU 2014:75), att ett antal bestämmelser i lag och förordning som endast anger att myndighet får fatta automatiserade beslut ska utmönstras eftersom de felaktigt fått myndigheter att tro att regleringen ska tolkas motsatsvis så att andra typer av beslut än de som omfattas av en sådan särbestämmelse inte får fattas automatiserat. I en lagrådsremiss infördes emellertid istället en generell regel om att beslut får fattas automatiserat (se regeringens proposition 2016/17:180 En modern och rättssäker förvaltning – ny förvaltningslag).

[25] När det gäller tillämpningsområdet för artikel 22 så gäller inte artikeln för beslutsfattande som har ett manuellt inslag. Det framgår inte helt tydligt om den automatiserade behandling på vilken beslutet grundas måste innefatta profilering för att bestämmelsen ska bli tillämplig, eller om ett beslut som fattas automatiserat utan profilering också kan omfattas av regeln. Att motsvarande bestämmelse i dataskyddsdirektivet enbart gäller för automatiserat beslutsfattande som innefattar profilering talar emot att dataskyddsförordningens bestämmelse skulle ha ett långt mer omfattande tillämpningsområde. Denna bedömning har också gjorts av Socialdataskyddsutredningen, se SOU 2017:66, s 273.

[26] Om en annan lag eller en förordning innehåller någon bestämmelse som avviker från förvaltningslagen ska emellertid, enligt 4 § förvaltningslagen (2017:900), den bestämmelsen tillämpas. Det innebär att andra regler kan gälla inom särskilda områden.

[27] Regeringen har gjort denna bedömning i prop. 2017/18:95, Anpassningar av vissa författningar inom skatt, tull och exekution till EU:s dataskyddsförordning, s 100. Se även eSams rättsliga uttalande den 19 mars 2018 Automatiserade beslut enligt EU:s dataskyddsförordning är tillåtna med stöd av förvaltningslagen.

3. Översikt över de juridiska förutsättningarna

Genom att i it-miljö knyta händelser och fakta till rättsregler, i enlighet med vedertagna juridiska synsätt och tolkningsmetoder, kan gällande rätt normalt tillämpas på ett fungerande sätt även i it-miljö.

3.1 Att tillämpa gällande rätt

Rättsregler knyts till vissa händelser eller fakta. Dessa inträffar numera också i it-system inom bl.a. e-förvaltningen. Den som utvecklar en it-baserad tjänst behöver redan från början beakta hur rättsreglerna förhåller sig till denna miljö. När jurister ska beskriva kombinationer av rättsregler, händelser och fakta använder de ofta uttrycket rättsfigur. En etablerad rättsfigur – dvs. en sådan som är allmänt godtagen – är en del av gällande rätt medan en ny och oprövad rättsfigur kan vara svår att tolka och tillämpa.

När nya it-baserade tjänster tas fram måste de rättsfigurer som de tekniska och administrativa lösningarna bygger på bedömas redan när arkitekturen utformas. Myndigheterna behöver samtidigt tillämpa rättsregler som kommit till för traditionell pappersmiljö på nya it-baserade förutsättningar. Det kan se annorlunda ut i dessa digitala flöden. Därför finns det en risk för att det som utvecklas inte blir rättsenligt. Numera har dock exempelvis eget utrymme och egen hämtning utvecklats till etablerade rättsfigurer. Regeringen har också förklarat att det finns stöd i praxis för att myndigheterna tillhandahåller digitala tjänster som uppfyller kraven i 2 kap. 10 § första stycket TF och att myndigheterna kommer att kunna utveckla och anpassa sina tjänster efter eventuell ytterligare rättspraxis eftersom de själva beslutar om utformningen av sina tjänster (prop. 2016/17:198 s. 16). Detta gör det vanligtvis möjligt att tillämpa gällande rätt på ett fungerande sätt genom att knyta händelser och fakta till rättsregler i enlighet med vedertagna juridiska synsätt och tolkningsmetoder.

3.2 Reglering som berörs

Detta avsnitt ringar in ett antal rättsområden som berörs eller kan komma att aktualiseras vid verksamhetsutveckling inom e-förvaltning.

Det är till stor del samma rättsfrågor som uppkommer i varje utvecklingsprojekt när rättsregler som har kommit till för traditionell pappersmiljö ska tillämpas på it-baserade tjänster. För jurister blir många av de rättsliga bedömningarna självklara.[28] Andra rättsfrågor behöver övervägas i samverkan mellan jurister och de som utvecklar tjänsterna för att det enklaste och bästa alternativet ska kunna väljas. Vår beskrivning av it-arkitekturer och rättsfigurer för elektronisk förvaltning ska därför inledas med en kort redovisning och bedömning av centrala rättsfrågor samt angreppssätt vid utvecklingen av it-baserade tjänster.

[28] Som exempel kan nämnas att en myndighet inte får lagra fler uppgifter om enskilda än vad som krävs för att myndigheten ska kunna utföra sitt uppdrag och att myndigheten inte får bereda sig tillgång till en enskilds eget utrymme eller dator eller använda sig av personuppgifter för ändamål som är oförenliga med dem för vilka uppgifterna samlades in.

- **Legalitetsprincipen:** Myndigheter behöver säkerställa att deras it-baserade tjänster faller inom ramen för myndighetens uppdrag (legalitet) och har stöd i rättsordningen.

- **Offentlighet- och sekretess:** Hanteringen av uppgifter i en it-baserad tjänst bör inte
  - resultera i att uppgifter som innehavaren ser som sina privata blir allmänna och offentliga handlingar (jfr eget utrymme),
  - utformas så att handlingar som sänds från en it-baserad tjänst och mottas i myndighetens mottagningsfunktion blir allmänna handlingar på ett stadium där det inte varit avsett, och
  - omgärdas av bristfälligt skydd så att sekretessen inte upprätthålls.

En myndighet som tillhandahåller en it-baserad tjänst med stöd av ett föreskrivet undantag från vad som är allmän handling bör vidta åtgärder för att säkerställa att tjänsten hanteras så att undantaget gäller. Tillhandahåller en myndighet eget utrymme åt enskilda bör tydliga förbud införas för befattningshavare mot att ta del av eller att annars använda innehållet i en enskilds eget utrymme och ändamålsenliga tekniska tillträdesbegränsningar finnas.

- **Förvaltningsrättsliga frågor:** En it-baserad tjänst bör
  - inte utformas så att utkast i eget utrymme anses ha kommit in enligt förvaltningslagen till den myndighet som tillhandahåller det egna utrymmet,
  - utformas så att kvittens sänds när en försändelse har kommit till den mottagningsfunktion som myndigheten anvisar och att felmeddelande lämnas om myndigheten inte kan läsa en mottagen försändelse, och
  - i eget utrymme kunna förenas med automatiserade kontroller, t.ex. en beloppsgranskning, så att innehavaren av utrymmet ges stöd när handlingar mottas, skapas och skickas.

- **Säkerhetsskydd:** När en myndighet planerar utformningen av en it-baserad tjänst måste myndigheten analysera om tjänsten kan komma att behandla information som omfattas av Säkerhetsskyddslagstiftningen.[29] Den tar sikte på skydd av hemliga uppgifter[30] och innehåller bestämmelser om säkerhetsåtgärder som ska vidtas till skydd för dessa uppgifter. Hemliga uppgifter har ett så starkt skyddsvärde att dessa uppgifter inte är lämpliga att hantera i publika e-tjänster. Denna vägledning tar därför inte hänsyn till eventuella regler som följer av säkerhetsskyddslagstiftningen. Myndigheten behöver säkerställa att hemliga uppgifter inte kommer att behandlas i en tilltänkt tjänst.[31]

- **Dataskydd:** När en it-baserad tjänst byggs behöver
  - den tekniska utformningen i sig ge skydd för enskildas personliga integritet (s.k. inbyggd integritet eller privacy by design),
  - personuppgiftsansvarets fördelning beaktas redan när funktionerna utformas,

[29] Säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633). – Regeringen har den 15 februari 2018 överlämnat propositionen 2017/18:89 Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag.
[30] Uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) och som rör rikets säkerhet.
[31] I detta sammanhang behöver även frågor om krisberedskap och civilt försvar beaktas. Exempelvis behöver risken beaktas för att kompetens och resurser avvecklas över tid, vilket kan få en avsevärt negativ påverkan på möjligheten att aktivera manuella reservrutiner i händelse av kris. Frågor om prioriteringar vid höjd beredskap eller krig behöver också beaktas.

- en analys av hot och sårbarheter och vilka säkerhetsåtgärder som behöver vidtas, göras som en integrerad del av utvecklingsarbetet, och omfatta hela den tänkta infrastrukturen,
- tjänsten utformas så att den eller de personuppgiftsansvariga kan uppfylla samtliga krav i EU:s dataskyddsförordning och i dataskyddslagen och dataskyddsförordningen samt i berörda registerförfattningar (i registerförfattningar är bl.a. ändamålsbestämmelser och bestämmelser om direktåtkomst viktiga att beakta), och
- personuppgiftsbiträdesavtal upprättas med berörda aktörer.

- **Information och samtycke:** Den information som måste lämnas enligt lag är omfattande och bör samlas så att den blir enkel att ta del av. Om en tjänst kan bygga på att samtycke ges, beträffande personuppgiftsbehandling eller för att sekretessreglerade uppgifter ska få lämnas ut, måste rutinerna för samtycke utformas så att giltiga samtycken uppkommer.
- **Säkerhetsåtgärder:** Varje aktör är ansvarig för att utforma och vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda sin information och för att åstadkomma en lämplig säkerhetsnivå, se vidare kap. 5.
- **Bevarande och gallring:** För att andra inte ska kunna få tillgång till information som en enskild ser som sin egen och att den enskilde inte ska kunna övervakas med hjälp av uppgifter som registreras i tjänsten kan omedelbar gallring behöva beslutas med avseende på handlingar som blivit allmänna. Gallring får beslutas endast om det finns stöd för det och bara av ett behörigt organ. Det är många fler åtgärder än radering som kan resultera i gallring. Det krävs särskilt beslut för att få gallra. Arkivlagstiftningen gäller endast för allmänna handlingar, se vidare Riksarkivets råd och vägledningar som finns tillgängliga på https://riksarkivet.se/vardera-och-gallra.
- **Författningsändringar eller avtal:** En myndighet som ska införa en ny it-baserad tjänst behöver överväga om det krävs ändringar i lag eller förordning för att göra tjänsten förenlig med författningsregleringen och om myndigheten till och med bör begära av regeringen att få utfärda egna föreskrifter. Myndigheten behöver vidare bedöma om den närmare regleringen av tjänsten ska ges genom avtal, normgivning eller förvaltningsbeslut för enskilda fall. Myndigheter under regeringen kan inte ingå civilrättsligt bindande avtal med varandra eftersom de är en del av samma juridiska person.
- **Utkontraktering (outsourcing):** En myndighets ansvar enligt reglerna om handlingsoffentlighet, sekretess samt bevarande och gallring gäller naturligtvis även när myndigheten använder sig av en tjänst för teknisk bearbetning och teknisk lagring som en underleverantör ställer till myndighetens förfogande (extern it-drift)
- **Upphandling, konkurrens, m.m.:** Reglerna om upphandling, konkurrens och immaterialrättsligt skydd måste följas.

4. Rättsfigurer för elektroniska tjänster

Här redovisas hur rättsfigurer kan brukas i elektroniska tjänster på ett rättsenligt sätt och hur dessa hör samman med vissa it-arkitekturer.

4.1 Allmän beskrivning av rättsfigurer

När gällande rätt ska tillämpas i it-miljö knyts som framgått vissa händelser och fakta till rättsregler så att rättsfigurer etableras. Dessa rättsfigurer kan i it-miljö förenklat beskrivas så att de

- i vissa fall återskapar viss plats, om en rättsregel har kommit till utifrån behovet av att
  - slå fast en tidpunkt eller en gräns för när en elektronisk handling har kommit dit, eller
  - ge rättsligt skydd för elektroniska handlingar som hanteras där,
- i andra fall inordnar vissa procedurer under gällande rätt, för att den rättsliga grunden för rättshandlingar och annan hantering ska bli tydlig och att rättsföljder ska inträda i enlighet med vedertagna juridiska synsätt.

4.1.1 Mottagningsfunktion

En mottagningsfunktion är en rättsfigur som fått stor spridning och rör viss (virtuell) plats, genom att klargöra när proceduren för att ge in en handling till en organisation anses ha nått så långt att handlingen ses som inkommen där enligt förvaltningslagen. Med mottagningsfunktion menas således en funktion för att ta emot en handling. Ibland svarar funktionen också med bevis om att handlingen har kommit in till den som tillhandahåller tjänsten.

Den juridiska frågan om inkommande handlingar genomlystes redan år 2005 av E-nämnden och en myndighetspraxis har vuxit fram med stöd av E-nämndens vägledning för hantering av inkommande elektroniska handlingar (se fotnot 9). Den 1 juli 2018 träder emellertid förvaltningslagen (2017:900) i kraft. Där föreskrivs såvitt här är av intresse att en handling har kommit in till en myndighet den dag som handlingen når myndigheten. Den nya regleringen innebär enligt eSams bedömning att en elektronisk handling, på motsvarande sätt som idag, anses komma in till en myndighet den dag handlingen når den funktion där myndigheten tar emot sådana handlingar. De tolkningsfrågor som aktualiseras har genomlysts av eSams rättsliga expertgrupp i en promemoria och ett rättsligt uttalande från oktober 2017.

4.1.2 Hämtning – tillgänglighet – gallring

Andra rättsfigurer, som fått en mer begränsad spridning, tar sikte på hur modern infrastruktur kan användas för att visa eller använda uppgifter utan att enskildas personliga integritet eller företagens intressen av skydd för sina uppgifter blir åsidosatta till följd av att en myndighetsgräns måste passeras.

En rättsfigur av detta slag är myndighets omedelbara hämtning; dvs. att en uppgift eller en handling hämtas in i realtid till en myndighet med stöd av en bastjänst så att den blir allmän handling där. Den kombineras ofta med rättsfiguren tillfällig tillgänglighet; dvs. att uppgifter eller handlingar under ett ögonblick eller en snävt avgränsad tid görs tillgängliga för en mottagande myndighet med en metod för tillträdesbegränsning och behörighetskontroll som begränsar överskottsinformationen så att endast det som ska användas i det enskilda fallet görs tillgängligt för mottagaren.[32]

Hit hör också en rättsfigur som blivit tydligt etablerad och fyller en betydelsefull praktisk funktion, särskilt när eget utrymme inte kan användas, nämligen omedelbar gallring eller rensning;[33] dvs. att uppgifter som i tryckfrihetsförordningens mening har kommit in till eller annars förvaras hos en myndighet genast raderas eller annars görs otillgängliga för att skydda informationen (se prop. 2016/17:198 s. 24).

4.1.3 Insynsskyddad elektronisk plats, egen hämtning och egen delning

En annan rättsfigur, som fått stor spridning och som efter regeringens uttalanden i lagmotiv får anses vara etablerad, är som framgått eget utrymme. Det syftar till att ge rättsligt skydd för data som finns på en insynsskyddad elektronisk plats. Med eget utrymme avses ett skyddat förvar som tillhandahålls enligt 2 kap. 10 § första stycket TF endast som led i teknisk bearbetning eller teknisk lagring för annans räkning.[34]

Ett eget utrymme som används kortvarigt kallas eget utrymme för en session medan ett som har registrerats för en viss fysisk eller juridisk person, så att denne permanent kan bevara och i övrigt behandla uppgifter där, kallas ”konto”. Ett konto dit elektronisk post kan levereras kallas ”e-brevlåda”.

Ytterligare rättsfigurer som främst rör viss plats har tillkommit i syfte att ge enskilda skydd för uppgifter som de hanterar i eller i anslutning till eget utrymme, nämligen

- egen hämtning; dvs. att en innehavare av ett eget utrymme, från utrymmet begär uppgifter och får dem utlämnade direkt till sitt eget utrymme (egen hämtning har kommit till omfattande användning – se hur t.ex. Vidareförmedlingstjänsten för grundläggande uppgifter om företag, SSBTGU fungerar), och
- egen delning; dvs. att en innehavare av ett eget utrymme, genom en aktiv åtgärd eller automatiserat, överför uppgifter från utrymmet till ett annat eget utrymme.[35]

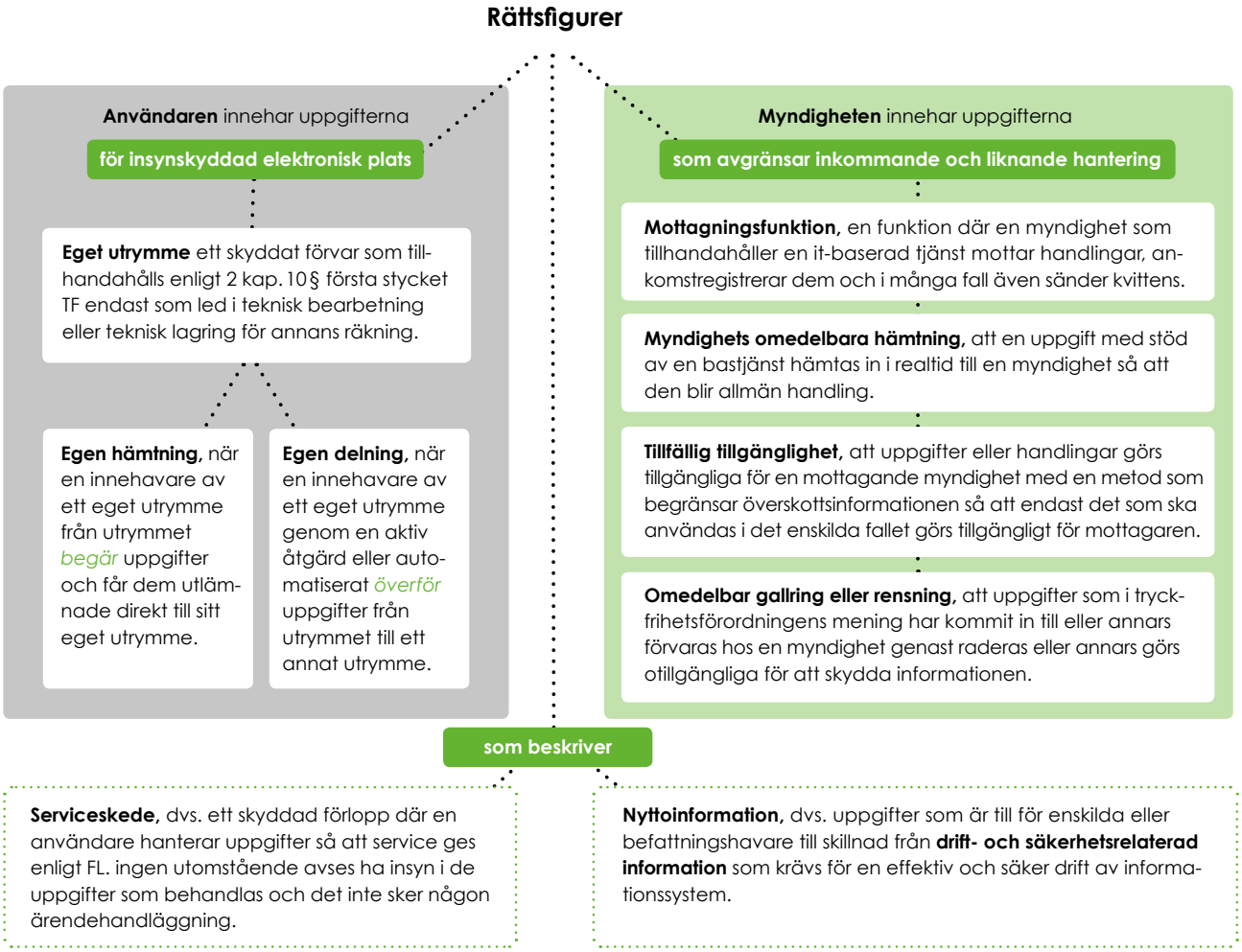
[32] Åtkomsten begränsas så i t.ex. en hjälpfunktion som Pensionsmyndigheten tillhandahåller åt Min Pension i Sverige AB.
[33] Rensning sker med avseende på handlingar som inte har blivit allmänna medan gallring avser handlingar som blivit allmänna och förutsätter särskilt beslut av behörig myndighet, se vidare Riksarkivets råd och vägledningar som finns tillgängliga på https://riksarkivet.se/vardera-och-gallra.
[34] Eget utrymme har i vissa sammanhang kallats elektroniskt förvar för att knyta an till regeln i 4 kap. 9 § brottsbalken om straffansvar för intrång i förvar (se SOU 2014:39). Regeringen använder dock begreppet eget utrymme (prop. 2016/17:198 s. 7).
[35] Funktioner för egen hämtning innebär således att användaren skickar en begäran så att automatiserat beslut om utlämnande fattas av annan myndighet (se t.ex. SSBTEK och LEFI Online) medan egen delning innebär att användaren skickar uppgifter från ett eget utrymme till ett annat. – I tidigare vägledningar talades även om egen visning. Egen hämtning och egen delning beskriver emellertid här hur uppgifter inhämtas. Att mottaget material kan sammanställas och läsas av den enskilde i ett serviceskede står klart utan att det behöver införas någon särskild term för det.

4.1.4 Serviceskede och nytto-, drift- och säkerhetsrelaterad information

I denna vägledning används uttrycket rättsfigur som samlingsbegrepp även för vissa andra samband mellan rättsregler och händelser eller fakta. Hit hör beskrivningen av ett s.k. serviceskede; dvs. ett skyddat förlopp där en användare hanterar uppgifter så att service ges enligt förvaltningslagen, ingen utomstående avses ha insyn i de uppgifter som behandlas och det inte sker någon ärende-handläggning.

Två andra samlingsbegrepp av betydelse för att beskriva juridiska förutsättningar är

- *nyttoinformation*, dvs. data som brukas av vanliga användare, till skillnad från
- *drift- och säkerhetsrelaterad information,* dvs. data som krävs för en effektiv och säker drift av informationssystem.[36]



Som framgått av sammanställningen kan dessa rättsfigurer delas in i tre kategorier; dels sådana där en enskild fysisk eller juridisk person innehar uppgifterna (grå ruta), dels sådana där myndigheten har uppgifterna (grön ruta), dels några samlingsbegrepp som beskriver vissa förhållanden (vita rutor, streckad ram). De rättsliga konsekvenserna av att använda dessa rättsfigurer beskrivs förenklat i det följande.

[36] Jfr SOU 2009:5 s. 109 och SOU 2014:39 bl.a. s. 27 och s. 30. Regeringen har anfört följande: ”För att inte de uppgifter som en användare sparar i sitt egna utrymme hos en myndighet ska bli en allmän handling krävs att myndigheten begränsar den egna personalens tillgång till uppgifterna. Myndighetens personal ska alltså endast hantera den drifts- och säkerhetsrelaterade informationen (prop. 2016/17:198 s. 14).

Eget utrymme: Handlingar i sådan miljö är med stöd av 2 kap. 10 § första stycket TF inte allmänna och skyddas där mot insyn av annan än innehavaren av utrymmet.

Egen hämtning och egen delning: Handlingar som görs tillgängliga på detta sätt i eget utrymme är enligt 2 kap. 10 § andra stycket TF inte heller allmänna.

Mottagningsfunktion: En funktion där rättslig tidpunkt framgår för inkommande enligt förvaltningslagen.

Tillfällig tillgänglighet: Information som tillgängliggörs på det här sättet tillgodoser genom inbyggt dataskydd bl.a. principen om uppgiftsminimering.

Omedelbar gallring eller rensning: Åtgärd som ger ett inbyggt dataskydd och säkerställer att handlingar förblir skyddade även när 2 kap. 10 § första stycket TF inte undantar dem från offentlighetsinsyn.

Serviceskede: Namn på den rättsliga grunden för myndighetens förfaranden innan handläggning av ett ärende sker. Den rättsliga grunden är myndighetens serviceskyldighet enligt förvaltningslagen.

4.2 It-arkitekturer samordnas med rättsfigurer

För it-baserade tjänster behövs också tekniska strukturer. I praktiken innebär detta att varje rättsfigur motsvaras och stöds av (delar av en eller flera) it-arkitekturer. Med it-arkitekturer brukar visserligen avses detaljerade tekniska beskrivningar. I denna vägledning redovisas emellertid som framgått övergripande (del-) strukturer och hur de kan samordnas med rättsfigurer inom ramen för gällande rätt.

På detta sätt kan samordnade it-arkitekturer och rättsfigurer stödja utvecklingen av tjänster.

5. Informationssäkerhet

För de myndigheter som lyder under förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap finns bestämmelser om vilket informationssäkerhetsarbete som en myndighet ska bedriva. Av särskild betydelse i detta sammanhang är de skyldigheter som följer av Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:01) som utfärdats med stöd av nämnd förordning. Där föreskrivs att en myndighet ska tillämpa ett ledningssystem för informationssäkerhet – i enlighet med etablerade standarder.

Detta innebär att myndigheten bland annat ska upprätta en informationssäkerhetspolicy, utse personer som leder och samordnar arbetet med informationssäkerhet, klassificera sin information, analysera risker och avgöra hur dessa ska hanteras, utvärdera informationssäkerhetsarbetet och besluta om förbättringsåtgärder samt genomföra och dokumentera granskningar. Motsvarande bör tillämpas av kommuner och landsting. Flertalet av de krav som redovisats är tillämpliga även vid verksamhetsutveckling, och som i detta fall vid utveckling av e-tjänster.

För att kunna bedöma vilka informationssäkerhetsåtgärder som ska vidtas med avseende på den information som behandlas i en e-tjänst behövs ett väl underbyggt beslutsunderlag så att åtgärderna utformas i proportion till de potentiellt negativa konsekvenser som kan uppstå om den information som behandlas i e-tjänsten görs åtkomlig för obehöriga, inte är korrekt eller inte är tillgänglig när den behövs. Ett sådant beslutsunderlag bör bestå i en rättslig analys, informationsklassificering, riskanalys och kravanalys.

I det följande redogörs för vilka aktiviteter som behöver genomföras för att sammanställa ett fullgott underlag inför ett beslut om vilken it-säkerhetsarkitektur och vilka informationssäkerhetsåtgärder som är lämpliga att införa för en e-tjänst.

5.1 Kartlägga informationsbehandling och samband

En förutsättning för att kunna bedöma vilka skyddsåtgärder som ska införas för en e-tjänst är att myndigheten har klarlagt vilken information som ska behandlas i tjänsten. Som utgångpunkt för en sådan bedömning bör myndigheten kartlägga vilka uppgifter som ska behandlas där, samt vilket inbördes förhållande uppgifterna har till varandra. För de myndigheter som tillämpar informationsarkitektur i sin verksamhet kan en sådan kartläggning bestå av en så kallad *informationsmodell.*

5.2 Rättslig analys

Med utgångpunkt i den informationskartläggning som myndigheten genomfört bör myndigheten undersöka vilka rättsliga krav som kan aktualiseras för den information som ska behandlas i tjänsten. I avsnitt 3.2 finns en förteckning över rättsfrågor som kan behöva beaktas.

5.3 Informationsklassificering

I 9 § Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:01) föreskrivs följande:

”I syfte att hantera hot och risker som rör informationssäkerheten i verksamheten ska myndigheten med stöd av modeller som myndigheten beslutar om klassa information med utgångspunkt i konfidentialitet, riktighet och tillgänglighet i olika nivåer utifrån vilka konsekvenser som kan uppstå av ett bristande skydd.”

Om myndigheten inte redan har gjort en informationsklassificering för den information som ska behandlas i e-tjänsten bör en sådan genomföras innan utvecklingen av e-tjänsten påbörjas.[37]

5.4 Riskanalys

När en e-tjänst planeras och utvecklas behöver det klarläggas vilka informationssäkerhetsrelaterade risker som är förknippade med den. En sådan riskanalys bör innefatta hela den kedja av informationsbehandlingar som blir aktuella när tjänsten införs och används. Ur ett rättsligt perspektiv kan analysen inte enbart begränsas till myndighetens egen it-miljö.[38]

5.5 Kravanalys

Resultatet av genomförd informationsklassificering, den rättsliga analysen samt riskanalysen läggs, tillsammans med de funktionella krav som verksamheten ställer, till grund för en analys av vilken it-säkerhetsarkitektur och vilka informationssäkerhetsåtgärder som är lämpliga för e-tjänsten. Syftet med kravanalysen är att säkerställa att de funktioner som e-tjänsten tillhandahåller omges av erforderliga skyddsåtgärder och att de harmonierar med de rättsliga krav som identifierats så att de informationssäkerhetsrelaterade riskerna minimeras. De skyddsåtgärder som vidtas i frågan om utveckling av en e-tjänst utgörs främst av tekniska skyddsåtgärder (exempelvis autentisering, kryptering, segmentering m.m.) men bör även vara av administrativ natur (exempelvis uppföljning och kontroll, behörighetsstyrning m.m.).[39]

5.6 Beslut om säkerhetsarkitektur och skyddsåtgärder

Utifrån kravanalysen ska skyddsåtgärder prioriteras och beslutas. Kravanalysen skickas lämpligen på en intern remiss inom organisationen innan beslut fattas. Lämpliga remissinstanser är företrädare för de verksamheter som berörs av e-tjänsten samt myndighetens rättschef och it-chef.

Beslut om åtgärder ska fattas i behörig ordning, exempelvis genom beslut av myndighetschefen eller annars i enlighet med myndighetens arbetsordning.

I syfte att hantera hot och risker som rör informationssäkerheten i verksamheten ska myndigheten med stöd av modeller som myndigheten beslutar om klassa information med utgångspunkt i konfidentialitet, riktighet och tillgänglighet i olika nivåer utifrån vilka konsekvenser som kan uppstå av ett bristande skydd.

[37] Metodstöd för informationsklassificering finns på Myndigheten för samhällsskydd och beredskaps webbplats. Se Modell för klassificering av information – rekommendationer (Publikationsnummer MSB 0040-09).
[38] Vägledning rörande vad som bör beaktas vid en riskanalys finns i den internationella standarden SS-ISO/IEC 27005 Riskhantering för informationssäkerhet. Se även HFD 2012 ref. 21 där frågan om personuppgiftsansvar vid tillhandahållande av elektroniska självbetjäningstjänster har berörts.
[39] Vägledning kring vilka informationssäkerhetsåtgärder som bör vidtas för en e-tjänst finns på olika håll. På en övergripande nivå, i fråga om skyddsförmågor, kan vägledning hämtas från den internationella standarden ISO/IEC 27002:2013 Informationsteknik – Säkerhetstekniker – Riktlinjer för informationssäkerhetsåtgärder samt Bilaga A i standarden SS-EN ISO/IEC 27001:2017 Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Krav.

6. Servicetjänster

6.1 Allmänt

6.1.1 Funktionalitet

1. Till servicetjänster hör it-arkitekturer för att innehavare av eget utrymme ska

   a. få hjälp så att

      i) uppgifter förifylls genom egen hämtning,

      ii) uppgifter överföras dit genom egen delning,

      iii) förklaringar och annat stöd ges utifrån tjänstens användningsområde,

      iv) handlingar kan skickas till en mottagningsfunktion,

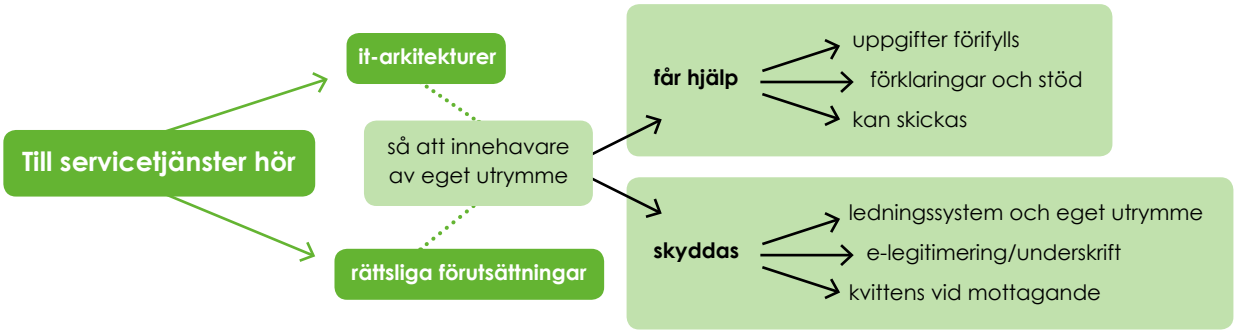
   b. skyddas i servicetjänsten – tekniskt, administrativt och rättsligt – genom ett

      i) väl avvägt it-säkerhetsskydd grundat i en riskanalys,

      ii) eget utrymme som tillhandahållaren av servicetjänsten utformat så att ingen annan än innehavaren av utrymmet får del av den nyttoinformation som finns i utrymmet,

      iii) system för legitimering, underskrift[40] och behörighetskontroll, och

      iv) kvittensförfarande när användare sänder handlingar; jfr följande figur.



2. Ett eget utrymme innehas normalt av den användare som har legitimerat sig för tillträde. Betjänar en servicetjänst företag kan myndigheten emellertid välja om den fysiska person som legitimerar sig för tillträde (användaren) eller den juridiska person som företräds (företaget) ska tilldelas utrymmet.[41] Vilket alternativ som tillämpas i det enskilda fallet beror på hur tillhandahållaren valt att utforma utrymmet och servicetjänsten (se avsnitt 6.4).

[40] Se beträffande denna hantering eSams publikation Juridisk vägledning för införande av e-legitimering och e-underskrifter.
[41] Drivs företaget som enskild firma är användare och företag samma rättssubjekt så att den fråga som här berörs inte blir aktuell.

6.1.2 Juridisk utformning

Grundläggande rättsfigurer

1. Redan i definitionen av servicetjänst anges att den bygger på rättsfiguren eget utrymme. Där behandlar innehavaren nyttoinformation i ett serviceskede, se avsnitt 2.1 om hur en servicetjänst förhåller sig till en presentationstjänst.

2. Eget utrymma finns numera beskrivet även i lagmotiv, se vidare eSams rättsliga uttalande den 22 november 2017 Eget utrymme hos myndighet och en promemoria den 22 november 2017 Eget utrymme är numera accepterat i lagmotiv – men vilka juridiska krav ställs på eget utrymme?[42]

3. Servicetjänsten kombineras med en mottagningsfunktion till vilken innehavaren av utrymmet kan skicka handlingar och få kvittens när en handling har kommit in enligt förvaltningslagen till myndigheten.

   Tillhandahållaren av servicetjänsten inför automatiserade procedurer för att adressera meddelanden till den mottagningsfunktion som används för försändelser från berört eget utrymme, se vidare eSams rättsliga uttalande den 26 oktober 2017 Ankomstdag för elektroniska handlingar och en promemoria den 31 oktober 2017 inkommandetidpunkt – när har en handling kommit in till myndighet?

Verkningar och avgränsningar

4. Den som brukar en servicetjänst hanterar informationen i ett eget utrymme, oberoende av om tillhandahållaren av tjänsten eller någon annan i detta serviceskede lämnat uppgifter till utrymmet eller om innehavaren av utrymmet mellanlagrar uppgifter och handlingar där, t.ex. för att i ett senare skede göra handlingen färdig och skicka in den. På detta sätt skyddas innehavaren av utrymmet från att myndighetens personal eller någon annan olovligen tar del av eller annars får tillgång till utkast eller annan nyttoinformation som finns i eget utrymme.

5. Utkast och andra handlingar som den enskilde hanterar i sitt eget utrymme anses inte vara inkomna enligt förvaltningslagen till den myndighet som tillhandahåller servicetjänsten. De kommer inte in förrän de har skickats av innehavaren till mottagningsfunktionen.

6. It-arkitekturen och de ändamål för vilka den används ska utformas så att nyttoinformation som innehavaren har i sitt eget utrymme förvaras där endast som led i teknisk bearbetning eller teknisk lagring för innehavarens räkning, se vidare avsnitt 2.6 om vilka krav som ställs på eget utrymme.

   En teknisk möjlighet, för den myndighet som tillhandahåller utrymmet, att komma åt en handling som finns där, leder alltså inte till att nyttoinformation i eget utrymme blir allmän handling, när utrymmet har utformats på ett ändamålsenligt sätt.

7. Det stöd och de kontroller som byggs in i eget utrymme som en service åt innehavaren ska ta sikte bara på material som inte har skickats från servicetjänsten, dvs. på handlingar som inte kommit in till myndigheten enligt förvaltningslagen eller tryckfrihetsförordningen.

It-arkitekturen och de ändamål för vilka den används ska utformas så att nyttoinformation som innehavaren har i sitt eget utrymme förvaras där endast som led i teknisk bearbetning eller teknisk lagring för innehavarens räkning

[42] http://esamverka.se/stod-och-vagledning/rattsliga-uttalanden/eget-utrymme.html, se även E-nämndens vägledning för hantering av inkommande elektroniska handlingar (e-nämnden 05:02) och Per Furberg i Svensk Juristtidning, Inkommande handlingar – en IT-anpassad tolkning (SvJT 2005, s. 273 ff.).

8. Servicetjänsten får inte utformas så att det kan uppkomma tvekan om när viss nyttoinformation lämnat det egna utrymmet och kommit in till myndigheten, se vidare eSams ovan nämnda rättsliga uttalande och promemoria om inkommandetidpunkten.[43]

6.2 Alternativ utformning av tjänsten

1. Servicetjänster kan utformas för att användas på olika sätt;

    a. antingen utan att

        i) den som tillhandahåller tjänsten fyller i eller annars lämnar ut uppgifter som behöver skyddas,

        ii) den enskilde behöver identifieras för att få tillträde till tjänsten,

    b. eller med

        iii) e-legitimering för att ges tillträde till tjänsten,

        iv) förifyllning eller annat utlämnade av uppgifter till eget utrymme, och

        v) egen hämtning eller egen delning till eget utrymme.

2. Servicetjänster kan också utformas olika för det stadium när en användare är färdig att skicka,

    a. antingen så att användaren behöver

        i) legitimera sig för uppgiftslämnande, eller

        ii) skriva under elektroniskt, och

        iii) få sin juridiska behörighet att utföra åtgärden kontrollerad,

    b. eller så att användaren varken behöver legitimera sig på nytt eller skriva under och inte heller behöver behörighetskontrolleras, t.ex. för att de kontroller som redan skett vid legitimering för tillträde anses tillräckliga också för att skicka handlingar till myndighetens mottagningsfunktion.

3. I eget utrymme kan finnas bastjänster för

    a. egen hämtning så att innehavaren av utrymmet därifrån kan begära uppgifter och få uppgifter utlämnade direkt till sitt eget utrymme,

    b. egen delning så att innehavaren av utrymmet, genom en egen aktiv åtgärd eller automatiserat, kan överföra uppgifter därifrån till ett annat eget utrymme,

    c. äkthetshantering så att användaren kan legitimera sig för uppgiftslämnande eller skriva under elektroniskt, och

    d. behörighetskontroll så att användare kan lämna bevis om sin rätt att agera för annans räkning.

[43] http://esamverka.se/stod-och-vagledning/rattsliga-uttalanden/inkommandetidpunkt.html, se även E-nämndens vägledning för hantering av inkommande elektroniska handlingar (e-nämnden 05:02) och Per Furberg i Svensk Juristtidning, Inkommande handlingar – en IT-anpassad tolkning (SvJT 2005, s. 273 ff.).

4. Till en servicetjänst kan också höra funktioner för att innehavare av eget utrymme ska kunna ta emot t.ex. myndighetens begäran om komplettering eller beslut, se vidare avsnitt 6.5 om de vidareförmedlingstjänster som etablerats för att förenkla användningen av bl.a. servicetjänster.

6.3 Alternativ från juridiska utgångspunkter

1. På samma sätt som när

    1. en myndighet i pappersmiljö skickar ut en förifylld blankett, kan en myndighet lämna ut en förifylld elektronisk handling till den enskildes eget utrymme,

    2. en enskild i pappersmiljö skaffar en handling från en myndighet för att ge in den till en annan myndighet, kan innehavare av eget utrymme genom egen hämtning med stöd av en bastjänst i ett serviceskede hämta uppgifter eller handlingar från någon annan till sitt eget utrymme,

    3. en fysisk person eller ett företag kan hantera sina handlingar i olika lokaler, kan innehavare av ett eget utrymme genom egen delning överföra uppgifter från ett annat eget utrymme med stöd av en bastjänst i ett serviceskede.

En förutsättning är dock att tillhandahållaren av utrymmet förvarar uppgifter, som t.ex. förifylls, hämtas eller delas med annat utrymme, endast som led i teknisk bearbetning eller teknisk lagring för utrymmesinnehavarens räkning (2 kap. 10 § första stycket TF).

2. För att uppgifter automatiserat ska få förifyllas eller annars lämnas ut till ett eget utrymme måste en sekretessprövning göras på förhand, när berörda uppgifter är sekretessreglerade. Detta gäller oberoende av om informationsutbytet sker genom egen hämtning, egen delning eller att uppgifter förifylls av den som tillhandahåller utrymmet.

    1. En sådan prövning blir normalt enkel om uppgifterna rör den enskilde själv och säkerheten är betryggande. Det kan dock finnas hinder i registerförfattning mot utlämnande till eget utrymme om användaren agerar som ombud för en fysisk person (se Högsta förvaltningsdomstolens dom den 4 dec 2017 i mål nr. 3716-16).

    2. Det kan också finnas hinder i en registerförfattning om den särskilt reglerar elektroniskt utlämnande i form av direktåtkomst eller utlämnande på medium för automatiserad behandling. En myndighet bör utforma sitt informationsutbyte så att direktåtkomst inte uppkommer (se HFD 2015 ref. 61 och eSams publikation Elektroniskt informationsutbyte – en vägledning för utlämnande i elektronisk form).

3. Enligt regeringens uttalanden i lagmotiv kan ett och samma informationsinnehåll finnas både i eget utrymme (utan att vara allmän handling där), och i myndighetens verksamhetssystem (som allmän handling där), se avsnitt 2.5 vid not 17.

Enligt regeringens uttalanden i lagmotiv kan ett och samma informationsinnehåll finnas både i eget utrymme (utan att vara allmän handling där), och i myndighetens verksamhetssystem (som allmän handling där)

4. En handling som kommit till eget utrymme genom egen hämtning eller egen delning blir alltså inte att anse som inkommen till den myndighet som tillhandahåller utrymmet, varken enligt förvaltningslagen eller tryckfrihetsförordningen. Detta gäller oberoende av om utrymmet bara används för en session eller för att bevara uppgifter för utrymmesinnehavarens räkning.

5. Vid egen hämtning kan handlingar begäras av användaren från ett eller flera organ, t.ex. för att

    1. uppgifter enkelt ska kunna föras in i ett utkast till en inlaga, eller

    2. handlingar ska kunna

        a. biläggas vid ingivning till myndigheten,

        b. förses med en elektronisk underskrift eller en elektronisk stämpel, eller

        c. ges in i samband med legitimering för uppgiftslämnande

Den som brukar mer än ett eget utrymme kan uppnå motsvarande förenklingar genom egen delning.

6. Oavsett vilket alternativ som väljs ska den information som hämtas och förvaras i eget utrymme inte bli allmän handling hos den myndighet som tillhandahåller utrymmet. Hanteringen måste därför vara utformad så att undantaget i 2 kap. 10 § första stycket TF blir tillämpligt, se avsnitt 2.6.

7. En servicetjänst kan också – utan ingivning till myndighet – brukas av innehavaren för att sammanställa och ta del av information i ett serviceskede. Användaren hämtar med stöd av bastjänster uppgifter eller handlingar till sitt eget utrymme från andra organ (egen hämtning eller egen delning) och får uppgifterna sammanställda automatiserat, utan att sammanställningen blir allmän handling.[44]

8. När beskrivna funktioner utformas måste gränsen vara tydlig mot åtgärder som anses vara en del av handläggningen av ett ärende och mot informationsutbyte som innebär direktåtkomst.

6.4 Ett eller flera utrymmen – användare eller företag som innehavare

6.4.1 Sortering av frågorna

1. En myndighet kan tillhandahålla flera olika servicetjänster. Därför kan en användare eller ett företag tilldelas flera egna utrymmen hos en och samma myndighet. Dessa utrymmen kan ha olika utformning.

    1. Ett eget utrymme som används kortvarigt betecknas eget utrymme för en session.

    2. Ett eget utrymme där uppgifter kan bevaras och i övrigt behandlas över tid kallas konto.
    – Ett konto dit elektronisk post levereras kallas e-brevlåda.

2. Ett eget utrymme innehas vanligtvis av den användare som har legitimerat sig för tillträde. När servicetjänsten är till för företag kan dock antingen

[44] Den enskildes enda avsikt med en sådan användning kan vara att få del av sammanställningen; jfr en presenta-tionstjänst. En förutsättning är emellertid även här att hanteringen utformats så att undantaget i 2 kap. 10 § första stycket TF blir tillämpligt.

användaren (dvs. den fysiska personen) eller företaget som användaren agerar för (dvs. den juridiska personen) tilldelas utrymmet.[45]

3. En myndighet som tillhandahåller servicetjänster behöver därför välja om

   a. nyttoinformation i eget utrymme ska rensas bort när en session är över (ett utrymme bara för en session) eller om nyttoinformation ska bevaras viss tid (ett utrymme som är ett konto),[46]

   b. en e-brevlåda ska ingå i ett konto eller om Mina meddelanden ska brukas för detta ändamål,[47]

   c. en myndighet som tillhandahåller flera olika servicetjänster med eget utrymme ska anses tillhandahålla ett eget utrymme för varje servicetjänst eller om samma utrymme ska användas för flera av myndighetens tjänster, och

   d. ett utrymme som brukas för ett företags räkning ska tilldelas användaren eller företaget

6.4.2 Bedömning

4. Dessa frågor är normalt enkla att bedöma när ett eget utrymme tilldelas endast för en session eftersom ett nytt utrymme skapas varje gång en inloggning sker och utrymmet genast avslutas. Ett sådant utrymme kan knappast brukas för mer än en servicetjänst. Eftersom utrymmet rensas bort genast kan det inte heller fungera som brevlåda eller annars så att någon brukar det vid en senare tidpunkt. Det bör därför vara användaren som tilldelas ett sådant utrymme och det är normalt tillräckligt att de krav blir uppfyllda som har redovisats i avsnitt 2.4.

5. När det är fråga om konton blir det vanligtvis en lämplighetsfråga om ett eller flera utrymmen ska anses föreligga. Är det användare som ska ges stöd bör användaren tilldelas utrymmet. Är det juridiska personer som ska ges en överblick över sina ärenden eller bör den juridiska kunna välja vem som ska gå in och fortsätta arbetet bör företaget tilldelas det egna utrymmet.

6. Olika lagringstider och olika krav på t.ex. integritetsskydd och nivåer av identifiering och behörighetskontroll kan motivera att skilda utrymmen tillhandahålls för olika åtgärder.

6.5 Vidareförmedlingstjänster – sammansatta bastjänster

6.5.1 Utformning

1. Som beskrivits i avsnitt 2.4. har myndigheter utvecklat funktioner för att hämta in handlingar i realtid med stöd av bastjänster, även kallade API. Detta kan ske antingen genom myndighets omedelbara hämtning när uppgifter lämnas direkt till myndighetens verksamhetssystem (se avsnitt 4.1.2), eller genom egen hämtning eller egen delning när informationen lämnas till användares eller företags eget utrymme hos myndigheten så att uppgifterna smidigt kan återanvändas av utrymmesinnehavaren (se avsnitt 4.1.2).

---

[45] Drivs företaget som enskild firma är användare och företag samma rättssubjekt så att den fråga som här tas upp inte blir aktuell.
[46] Se vidare eSams publikation Eget utrymme hos myndighet – en vägledning.
[47] Ska en myndighets konton även innehålla en e-brevlåda behöver myndigheten avgöra om det ska finnas en e-brevlåda för varje konto eller om e-brevlådan ska tillhandahållas gemensamt för dessa.

2. Återanvändning där uppgifter förs till eget utrymme genom egen hämtning går till så att innehavaren av utrymmet begär uppgifter och att den eller de som avses lämna ut uppgifter mottar begäran, söker fram uppgifterna, ställer samman dem, prövar om de får lämnas ut och expedierar dem.

3. Bastjänster kan sättas samman till vidareförmedlingstjänster. Uppgifter hämtas från flera källor och lämnas

    a. antingen direkt till en myndighet så att myndigheten kan återanvända uppgifterna utan att någon annan behöver ge in dem på nytt,

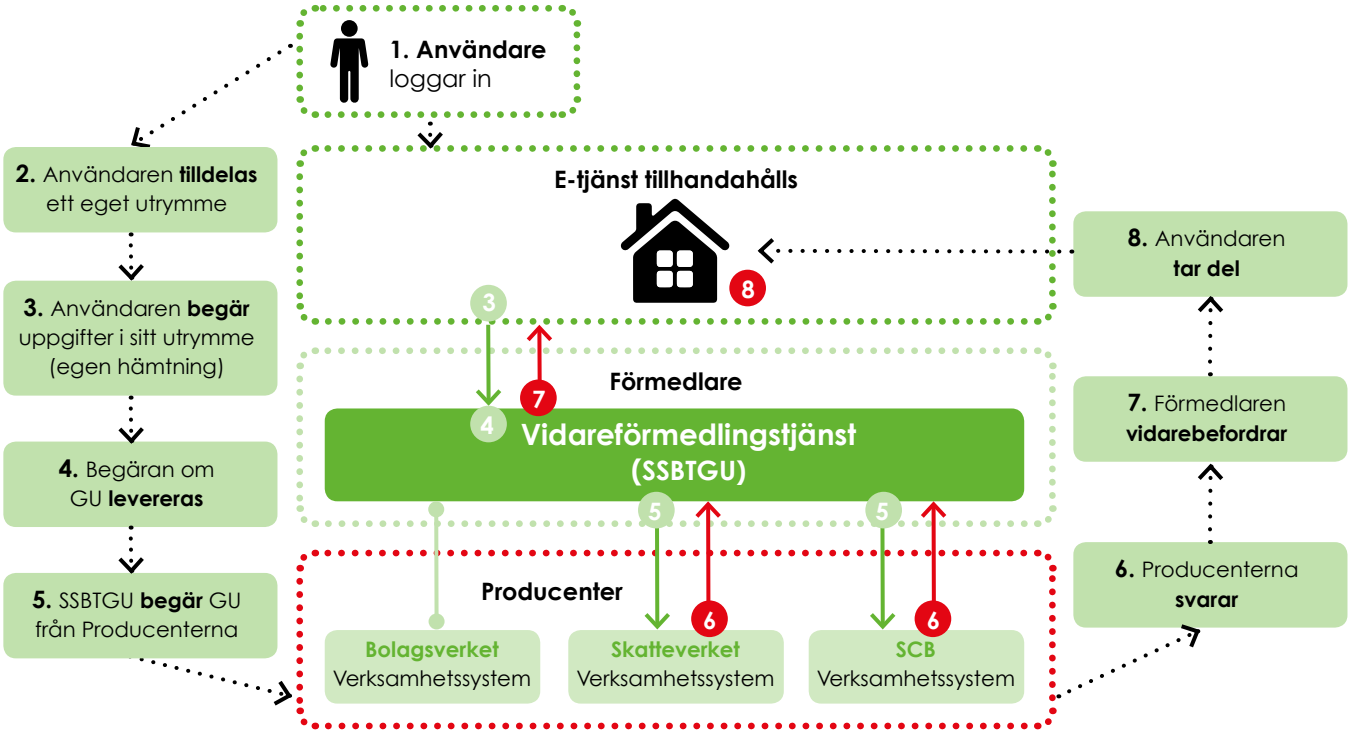
    b. eller till eget utrymme där innehavaren t.ex. får dem förifyllda i ett utkast till en ansökan eller annars förses med dem så att utrymmesinnehavaren enkelt kan ge in uppgifterna på nytt.[48]

Funktioner för återanvändning med stöd av en vidareförmedlingstjänst tillhandahålls redan för att underlätta hanteringen av ärenden om ekonomiskt bistånd (SSBTEK) samt inom Verksamt.se[49] och av myndigheter utanför Verksamt.se som har anslutit sina e-tjänster till Infrastrukturen för vidareförmedling av grundläggande uppgifter om företag, ofta kallad SSBTGU.[50] Vidareförmedlingstjänsten är således utformad för ett helt automatiserat utlämnande på medium för automatiserad behandling (se vidare avsnitt 2.7).

4. En vidareförmedlingstjänst bygger typiskt sett på att flera myndigheter (s.k. - producenter) lämnar ut uppgifter på begäran efter att automatiserat ha beslutat om ett utlämnande ska ske. Dessutom finns en aktör (den s.k. förmedlaren) som vidarebefordrar de frågor som ställs och vidarebefordrar de svar som lämnas till mottagaren som kan ta del av och använda uppgifterna.

Förfarandet när en vidareförmedlingstjänst används i eget utrymme kan gå till så att (1) en användare loggar in, (2) tilldelas ett eget utrymme som försetts med en vidareförmedlingstjänst, (3) begär uppgifter och att (4) begäran skickas till förmedlaren, (5) som levererar den till de myndigheter som lämnar ut uppgifter, producenterna. De (6) svarar efter att ha beslutat om utlämnande, (7) till förmedlaren, som (8) vidarebefordrar utlämnade uppgifter till det egna utrymme från vilket begäran sänts (8) där användaren tar del av och brukar uppgifterna, se figuren nedan.

[48] Denna utveckling ska förenkla för enskilda genom att de inte behöver ge in samma uppgift flera gånger och för myndigheter genom att tillförlitliga uppgifter hämtas från den bästa källan och ges in så att de kan godtas utan ytterligare granskning.
[49] Skatteverket, Tillväxtverket, Bolagsverket och Arbetsförmedlingen har inom ramen för Verksamt.se utvecklat och etablerat verktyg och tjänster för att fundera, starta, driva, utveckla och avveckla företag, vidareförmedla grundläggande uppgifter om företag, och samordna dessa verktyg och tjänster med it-baserade tjänster utanför Verksamt.se.
[50] Bolagsverket, Skatteverket oh Statistiska Centralbyrån har utarbetat denna infrastruktur och ett regelverk för den samt etablerat enhetliga förfaranden för indirekt återanvändning. Arbete pågår med motsvarande funktioner för direkt återanvändning, se http://www.bolagsverket.se/om/oss/samverkan/sammansatt-bastjanst/dokumentation-sammansatt-bastjanst-1.15560. När denna vägledning togs fram hade ett 40-tal myndigheter anslutit sina servicetjänster till denna infrastruktur.



5. Förfarandet är i princip detsamma när uppgifter begärs av och lämnas direkt till en myndighet, med undantag för att det inte är något eget utrymme inblandat och att de uppgifter som mottas genast blir allmän handling hos mottagaren. Bilden ovan förändras därvid endast så att det inte finns något eget utrymme och att det är myndigheten som begär uppgifterna och direkt mottar svaren.

6. It-baserade tjänster kan emellertid utformas på många andra sätt. Det som beskrivits här är endast exempel på hur bastjänster kan sättas samman för att förenkla enskildas uppgiftslämnande och förse myndigheter med tillförlitliga uppgifter som är hämtade från den bästa källan.

6.5.2 Juridiska aspekter

7. Förmedlaren agerar i egenskap av underleverantör åt de tillhandahållare av e-tjänst som har anslutit sig till vidareförmedlingstjänsten och hanterar uppgifter endast tekniskt. Den som tillhandahåller e-tjänsten erbjuder i sin tur vidareförmedlingstjänstens funktioner åt sina innehavare av eget utrymme. Producenterna agerar i eget namn i sin it-miljö där de mottar begäran, prövar den och lämnar ut uppgifter.[51]

8. Information som hämtas från flera myndigheter bör endast momentant göras tillgänglig hos en och samma myndighet. Även i övrigt bör uppgifterna hanteras på ett ändamålsenligt sätt så att 2 kap. 10 § första stycket eller 11 § första stycket 1 TF blir tillämpligt.

9. Krävs central lagring bör den så långt möjligt begränsas till hänvisningar och liknande underlag för att endast momentant ha fullständig information samlad, dvs. att den fullständiga informationen finns samlad endast när den

[51] Det som äger rum hos en producent, från mottagande av begäran till det att svar lämnas faller alltså utanför såväl området för användarens eget utrymme som tillhandahållare av e-tjänsts och förmedlarens hantering. Hanteringen bygger på sekundsnabba förlopp via vidareförmedlingstjänsten, där förmedlaren rensar bort de uppgifter som finns kvar där så snart en handling har vidareförmedlats via funktionerna för att förmedla uppgifter.

behövs och därefter snarast rensas eller gallras bort. Vidareförmedlingstjänsterna behöver utformas på ett ändamålsenligt sätt så att användare inte blir övervakade eller kartlagda (2 kap. 6 § andra stycket regeringsformen).

10. Vid återanvändning bör direktåtkomst undvikas. Finns hinder i en registerförfattning mot att lämna ut uppgifter från en myndighet till en annan kan det övervägas att lämna ut uppgifter till användarens eller företagets eget utrymme. Dessutom kan information, efter att den lämnats ut till eget utrymme göras tillgänglig för användaren eller företaget i annat eget utrymme efter egen delning.

11. Det kan finnas hinder i registerförfattning mot utlämnande till eget utrymme om användaren agerar som ombud för en fysisk person (se HFD:s dom den 4 dec 2017 i mål nr. 3716-16).

6.6 Säkerhetsarrangemang

1. För att ge användare och företag ett tillräckligt skydd vid hanteringen av uppgifter i eget utrymme behöver det från ett övergripande perspektiv övervägas vilka skyddsåtgärder som ska vidtas. Även straffrättsliga och civilrättsliga ansvarsförhållanden är betydelsefulla i detta sammanhang.

6.6.1 Av straffrättslig betydelse

2. En myndighet som inför en servicetjänst bör, genom noggrant utformade avtalsvillkor eller föreskrifter, förbjuda sin personal att bereda sig tillträde till nyttoinformation i någon annans eget utrymme. En sådan åtgärd blir därmed straffbar som dataintrång, utom i de sällsynta undantagsfall där åtgärden krävs av informationssäkerhetsskäl, för att rätta fel i myndighetens informationssystem eller för att verkställa ett straffprocessuellt tvångsmedel.

   Detta kan jämföras med att en fastighetsskötare som har huvudnyckel går in i en lägenhet endast när vattnet sprungit läck eller en annan nödsituation uppkommit.

3. Myndigheten bör också informera personal som självständigt sköter en kvalificerad teknisk uppgift eller övervakar en sådan att missbruk av denna förtroendeställning under vissa förutsättningar kan bli att anse som trolöshet mot huvudman.

4. En myndighet bör vidare, innan en servicetjänst införs, noga överväga vilka krav på underskrifter eller andra åtgärder i elektronisk form som bör ställas för att skydda myndigheten och användaren mot förfalskningar, bedrägerier eller andra manipulationer.[52] I vissa fall kan elektronisk underskrift med viss säkerhetsnivå anses nödvändig för att ta tillvara det straffansvar som numera gäller i elektronisk miljö för urkundsförfalskning och förnekande av underskrift, jfr Högsta domstolens dom den 22 december 2017 i mål T 435-17 rörande bl.a. bevisbördan i ett tvistemål vid en invändning om förfalskning.

5. Lägg märke till att en elektronisk underskrift på en handling och den underskrivna handlingens utseende blir av betydelse även när kopior ska spridas utan särskilt tekniskt äkthetsskydd, eftersom det är straffbart som

En myndighet bör vidare, innan en servicetjänst införs, noga överväga vilka krav på underskrifter eller andra åtgärder i elektronisk form som bör ställas för att skydda myndigheten och användaren mot förfalskningar, bedrägerier eller andra manipulationer.

[52] Se även E-delegationens vägledning den 7 juni 2012 Elektroniska original, kopior och avskrifter.

missbruk av handling att sanningslöst utge en handling för att vara en riktig kopia av viss urkund (se vidare 14 kap. 1 § och 15 kap. 12 och 13 §§ brottsbalken samt prop. 2012/13:74).

6.6.2 Av betydelse för ansvarsfördelningen

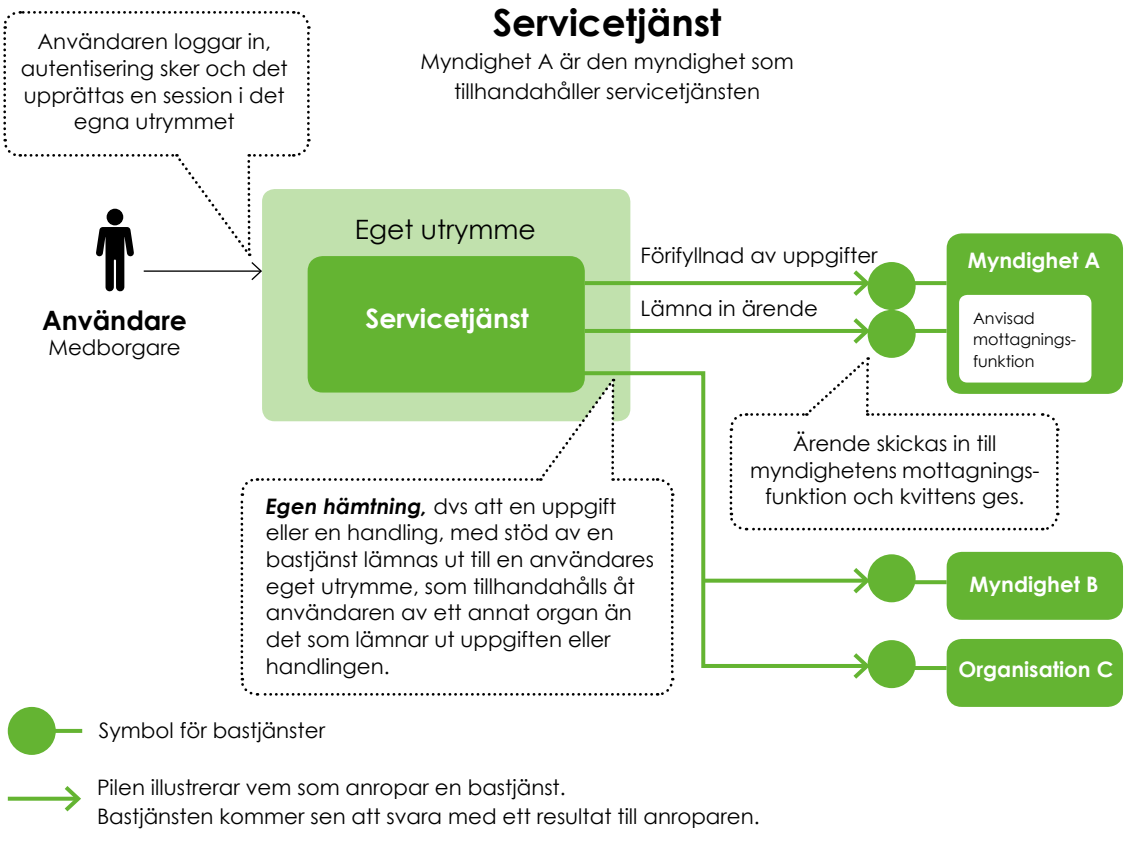
6. Det är den myndighet som tillhandahåller servicetjänsten som i egenskap av förlitande part står risken vid kontroller av användares identitet och behörighet att utföra rättshandlingar. Är det en annan person eller en obehörig person som utför åtgärden kan rättshandlingen visa sig sakna verkan mellan angivna parter. Enkelt uttryckt har den som pekats ut för att t.ex. ha anhängiggjort ett ärende eller svarat som motpart i ärendet inte utfört rättshandlingen. För fall av detta slag finns särskilda s.k. rättsmedel, så att juridiska fel kan rättas exempelvis så att ett beslut undanröjs när en obehörig har agerat.

7. Det är inte ovanligt att synnerligen höga säkerhetskrav föreslås i utvecklingsprojekt utan att det beaktats om säkerheten vid motsvarande ärendehantering på papper är låg. I andra fall kan skyddsbehovet ha underskattats. Det är viktigt att tidigt genomlysa vilket behov av skydd som finns och vilken aktör som står risken vid fel eller missbruk.

6.6.3 Grundläggande arrangemang för informationssäkerheten

8. Se kap. 5.

6.7 Arkitektur för servicetjänst



6.7.1 Servicetjänst

1. En session upprättas med en användare i ett eget utrymme. Med serviceskede menas ett förlopp från användarens inloggning till dess han eller hon ger in en handling till den myndighet som tillhandahåller utrymmet. Inom serviceskedet kan delförlopp förekomma där olika funktioner används. Här beskrivs från praktiska utgångspunkter några av de funktioner som används tillsammans med en servicetjänst och vilka förutsättningar som ska vara uppfyllda.

6.7.2 Eget utrymme

2. En servicetjänst ska utformas så att bara den autentiserade användaren får åtkomst till nyttoinformation i dennes utrymme. Undantag kan endast göras i de sällsynta undantagsfall där myndighetens tekniska personal måste utföra en åtgärd av informationssäkerhetsskäl, för att rätta fel i myndighetens informationssystem eller för att verkställa ett straffprocessuellt tvångsmedel. Denna begränsning får inte hindra teknisk förvaltning av tjänsten.

3. Ett eget utrymme i servicetjänsten kan utformas så att användaren själv kan hämta uppgifter (egen hämtning) hos en annan myndighet eller annan organisation via bastjänster.

4. Den information som hämtas till eget utrymme kan inte användas av myndigheten utan bara av användaren för att förifylla, bifoga eller annars använda den som ett led i serviceskedet.

5. Eget utrymme kan användas för att lagra information så att den finns kvar när sessionen är över. Ett syfte med eget utrymme är att den information som hanteras och utbyts där inte blir inkommen handling hos myndigheten. Myndigheten ska svara för informationssäkerheten i servicetjänstens alla delar, även för säkerheten i användarens eget utrymme.

6.7.3 Myndighetens omedelbara hämtning

6. Vid informationsutbyte via en servicetjänst kan en myndighet istället för egen hämtning välja att använda myndighets omedelbara hämtning (se avsnitt 4.1.2) Myndigheten hämtar då som aktör i realtid information från andra myndigheter. När myndigheten väljer detta förfarande kan myndigheten använda den information som hämtats även i andra sammanhang. Myndighets omedelbara hämtning är dock möjligt bara om det finns legala förutsättningar för detta förfarande. Skillnad mellan de olika metoderna egen hämtning och myndighets omedelbara hämtning är främst juridisk.

6.7.4 Förifyllnad av uppgifter, egen hämtning och kontroller

7. Förifyllnad av uppgifter i servicetjänsten kan ske genom att servicetjänsten hämtar information från myndighetens bakomliggande system. Det går att kombinera förifyllnad av uppgifter som är hämtade från den egna myndigheten med att hämta uppgifter från andra myndigheter och organisationer genom egen hämtning. Användaren kan komplettera med egen information i servicetjänsten. Kontroll av registrerade uppgifter kan ske i eget utrymme

som en service åt användaren. Detta sker mot myndighetens bakomliggande tjänster inom serviceskedet, utan att information i det egna utrymmet genom interaktionen blir allmän handling där.

6.7.5 Anvisat mottagningsställe

8. Anvisat mottagningsställe är en virtuell plats hos myndigheten med funktioner för att myndigheten ska kunna ta emot elektroniska handlingar. Det anvisade mottagningsstället är den ”elektroniska plats” som servicetjänsten pekar ut. Vid utformningen av användargränssnittet i servicetjänsten måste det vara tydligt för användaren om en åtgärd av denne leder till att handlingen skickas in till myndigheten eller om det istället handlar om att exempelvis spara ett utkast.

9. En myndighet bör så snart en elektronisk handling har nått myndighetens mottagningsfunktion logga inkommandet, förse handlingen med uppgift om när handlingen kom in till myndigheten och ge en mottagningskvittens till avsändaren.

Vid utformningen av användargränssnittet i servicetjänsten måste det vara tydligt för användaren om en åtgärd av denne leder till att handlingen skickas in till myndigheten eller om det istället handlar om att exempelvis spara ett utkast.

7. Presentationstjänster

7.1 Allmänt

1. Genom presentationstjänster, ofta kallade Mina sidor, visas uppgifter i eget utrymme för användare och företag utan att det som visas får blir tillgängligt för någon annan. Syftet är att ge en överblick över t.ex. vilka olika egna utrymmen som en användare eller ett företag innehar hos en eller flera myndigheter eller vilka ärenden som denne har anhängiggjort.

2. Uppgifter och handlingar som presenteras kan finnas i ett exemplar i myndighetens verksamhetssystem och i ett annat exemplar i användarens eller företagets eget utrymme (se avsnitt 2.5).

Genom presentationstjänster, ofta kallade Mina sidor, visas uppgifter i eget utrymme för användare och företag utan att det som visas får blir tillgängligt för någon annan.

7.1.1 It-arkitekturernas funktionalitet

Sättet för att samla in uppgifter

3. Uppgifter kan överföras till eget utrymme för en presentationstjänst

   a. från den som tillhandahåller tjänsten,

      i. direkt ur dennes egna informationstillgångar, eller

      ii. efter att denne begärt och fått uppgifter från annan för visningsändamål, eller

   b. från andra genom egen hämtning eller egen delning till eget utrymme i presentationstjänsten.[53]

4. Uppgifter som inte redan finns i verksamhetssystem hos den som tillhandahåller presentationstjänsten kan bl.a. genom vidareförmedlingstjänster begäras från annan momentant eller samlas in på förhand.

5. När uppgifter samlas in på förhand kan det ske till den myndighet som tillhandahåller presentationstjänsten eller till någon annan som fått i uppgift att lagra data. Uppgifter kan därefter begäras från den som lagrar dem när de behövs i en tjänst.

6. En presentationstjänst kan vara utformad så att användare bevarar uppgifter i eget utrymme. Det är emellertid av integritetsskäl sannolik olämpligt eller rent av förbjudet för en myndighet att över tid lagra omfattande information. Uppgifterna bör därför hämtas in momentant och omedelbart rensas bort från användarens eget utrymme efter att uppgifterna visats för denne i presentationstjänsten.

7. En presentationstjänst kan vara knuten till ett så stort antal leverantörer av uppgifter att momentan insamling kan vara svår att åstadkomma av prestandaskäl. Ett index kan därför behöva föras för varje användares eller företags eget utrymme som visar var relevant information kan begäras.

   En användares eller ett företags aktivitetsindexinformation kan lagras i dennes eget utrymme där den behandlas bara för användarens räkning. Användaren riskerar därmed inte att bli kartlagd eller övervakad eftersom informationen omfattas av sekretess enligt 40 kap. 5 § OSL.

[53] En handling kan därmed bli allmän hos en myndighet som tillhandahåller en presentationstjänst, för att myndigheten samlar in uppgifter i syfte att presentera dem i presentationstjänsten, men de kan också överföras direkt till användarens eget utrymme, från ett annat organs informationstillgångar eller ett eget utrymme där, jfr avsnitt Fel! Hittar inte r eferenskälla. om hur presentationstjänster förhåller sig till servicetjänster.

Med eller utan förhandsregistrering av användaren

1. En presentationstjänst kan antingen fungera utan registrering av användare på förhand, genom att de vid varje visningstillfälle, efter legitimering, får information om behandlingarna och lämnar samtycke till användarvillkor, eller förutsätta att användare av tjänsten har registrerats på förhand så att vissa uppgifter bevaras, t. ex. aktivitetsindexinformation.

2. De uppgifter som samlats in och sammanställts automatiserat ska hanteras så att åtkomst till materialet är utesluten för myndighetens personal, med undantag för åtkomst som är nödvändig för att åtgärda tekniska fel eller skydda mot angrepp eller annat missbruk (jfr avsnitt 2.6).

3. Uppgifter bör gallras så snart det kan ske (om de finns i myndighetens verksamhetssystem), respektive rensas bort genast (om de finns i eget utrymme), förutsatt att annat inte överenskommits med innehavaren av utrymmet och åtgärder vidtagits för att skydda uppgifterna över tid.

7.1.2 Juridisk utformning

Rättsfigurer

1. En presentationstjänst bygger på att en myndighet, som inte redan har berörda uppgifter hos sig,

    a. samlar in informationen, t.ex. genom myndighets omedelbara hämtning, – handlingar begärs och lämnas ut i realtid till en myndighet med stöd av bastjänster så att handlingarna blir allmänna hos den myndighet som samlar in dem, eller

    b. tillhandahåller funktioner i eget utrymme så att användare samlar in handlingar momentant till sitt utrymme genom egen hämtning eller egen delning, – handlingar lämnas i realtid till eget utrymme med stöd av bastjänster, så att inhämtade handlingar inte blir allmänna hos den som tillhandahåller eget utrymme för presentation.

2. Denna hantering behöver kombineras med omedelbar gallring så att handlingar raderas eller annars görs otillgängliga för myndigheten så snart det kan ske. Det som samlas in och sammanställs i en presentationstjänst är normalt av sådan tillfällig eller ringa betydelse att det får gallras efter beslut av den myndigheten som tillhandahåller tjänsten.[54]

3. Sker insamling på förhand till en annan myndighet eller en privaträttslig aktör för teknisk lagring där är det viktigt att en begäran om utlämnande prövas genom automatiserat beslut så att de handlingar som lagras hos annan inte kontinuerligt ska anses vara inkomna och förvarade och därmed allmänna handlingar även hos den begärande myndigheten (se avsnitt 2.7, HFD 2015 ref. 61 och eSams publikation Elektroniskt informationsutbyte – en vägledning för utlämnande i elektronisk form).

[54] Se prop. 2016/17:198 s. 24 och avsnitt 4.1.2 där det framgår att rättsfiguren omedelbar gallring numera är etablerad.

4. Det som hämtas till en myndighet blir normalt att anse som inkommet enligt tryckfrihetsförordningen och därmed som allmän handling hos myndigheten. För att undvika att samlingar av allmänna handlingar skapas när det inte är nödvändigt bör som framgått insamling på förhand undvikas.

5. Blir det ändå, av t.ex. tekniska eller administrativa skäl, nödvändigt att samla in uppgifter på förhand kan en annan myndighet eller ett privaträttsligt subjekt ges i uppgift att tekniskt lagra materialet.

6. Sker sådan insamling till annan behöver åtkomsten till materialet begränsas tekniskt för den myndighet som tillhandahåller presentationstjänsten, antingen genom att utlämnande endast sker på begäran efter automatiserat beslut (dvs. inte genom direktåtkomst) eller att den myndighet som tillhandahåller presentationstjänsten endast medges en tillfällig tillgänglighet till berörd information. Under det skede när tillgänglighet föreligger blir handlingarna nämligen att anse som allmänna hos den myndighet som har åtkomst till dem (se eSams publikation Elektroniskt informationsutbyte – en vägledning för utlämnande i elektronisk form).[55]

7. För att uppgifter automatiserat ska kunna hämtas genom myndighets omedelbara hämtning måste en sekretessprövning göras på förhand. En sådan prövning blir normalt enkel när ett utlämnande sker till eget utrymme, uppgifterna bara rör den enskilde själv och säkerheten är betryggande. Lägg märke att sekretess kan gälla mellan myndigheter även om uppgifter finns i eget utrymmen och lämnas ut till eget utrymme endast under förutsättning att mottagande myndighet inte får ta del av uppgifterna.

8. Det behöver kontrolleras om ett utlämnande blir att anse som direktåtkomst och – om så är fallet – huruvida direktåtkomst är tillåten enligt en berörd registerförfattning (se HFD 2015 ref. 61 och eSams publikation Elektroniskt informationsutbyte – en vägledning för utlämnande i elektronisk form).

9. Bygger visning som sker i en presentationstjänst på att användaren har ett konto behöver det övervägas om en sådan tjänst faller inom ramen för myndighetens uppdrag (legalitet) och hur länge uppgifter i så fall ska få lagras, dvs. när de måste rensas bort. Vad som ska vara tillåtet behöver också klargöras i kontovillkoren. Avses lagring ske behöver myndigheten dessutom överväga om detta kan förenas med skyddet för enskilda och vilka åtgärder och begränsningar som behöver införas för att funktionerna inte ska kunna missbrukas.

Bygger visning som sker i en presentationstjänst på att användaren har ett konto behöver det övervägas om en sådan tjänst faller inom ramen för myndighetens uppdrag (legalitet) och hur länge uppgifter i så fall ska få lagras, dvs. när de måste rensas bort.

7.2 Ett eller flera utrymmen – användare eller företag som innehavare

7.2.1 Sortering av frågorna

1. Myndigheter som tillhandahåller presentationstjänster tillhandahåller vanligtvis även servicetjänster. En användare eller ett företag kan därför, utöver eget utrymme för en presentationstjänst, ha tilldelats andra utrymmen i form av konton eller brevlådor, jfr avsnitt 6.4.

[55] Denna lösning används när Pensionsmyndigheten tillhandahåller en hjälptjänst åt Min pension i Sverige AB. Pensionsspararen måste samtycka till den tillfälliga åtkomst som Pensionsmyndighetens handläggare ges och när denna tid löpt ut stänger Min pension i Sverige AB myndighetens möjlighet att komma åt den pensionsspararens pensionsinformation hos bolaget.

2. Mina sidor och andra liknande presentationstjänster innehas normalt av den användare som har legitimerat sig för tillträde. Det kan emellertid inte uteslutas att presentationstjänster i vissa fall behövs för företag så att alla som är behöriga att ta del av uppgifter för företagets räkning kan logga in där.

3. En myndighet som tillhandahåller en presentationstjänst med eget utrymme behöver välja om

   a. eget utrymme för en presentationstjänst bör tilldelas användare eller företag,

   b. presentationstjänsten bör omfatta bara den myndighetens uppgifter eller om även information från andra myndigheter ska visas i presentationstjänsten,

   c. nyttoinformation i eget utrymme för en presentationstjänst bör rensas när en session är över eller om den ska finnas kvar i tjänsten,[56]

   d. eget utrymme bör tillhandahållas separat för varje presentationstjänst och servicetjänst eller om samma utrymme bör få brukas av en användare eller ett företag för flera tjänster, och

   e. den nyttoinformation och aktivitetsindexinformation som samlas in bör kunna distribueras till andra myndigheters presentationstjänster så att samlad information kan presenteras även där.[57]

7.2.2 Bedömning

4. Presentationstjänster bör normalt tilldelas användare så att de kan få en överblick över vad de har gjort och har kvar att utföra när de använder myndigheters it-baserade tjänster.

   Överväger en myndighet en presentationstjänst för företag behöver det på ett tidigt stadium genomlysas om tjänsten kan förenas med regler om juridisk behörighet, persondataskydd och sekretess.

5. För tillämpningen av 2 kap. 10 § första stycket TF är det inte av betydelse om ett eller flera utrymmen föreligger eller om ett utrymme tilldelas en användare eller ett företag. Avgörande är om uppgifterna hanteras endast tekniskt för utrymmesinnehavarens räkning.

6. Vid bedömningen av följande frågor blir det emellertid av betydelse om ett eller flera utrymmen föreligger och vem som har tilldelats ett utrymme.

   a. Tillhandahålls presentationstjänsten åt användare kan användaren överblicka sin hantering, men däremot inte den hantering som utförs av andra företrädare för berörd juridisk person.

   b. Från straffrättsliga utgångspunkter blir det av betydelse för tillämpningen av bl.a. bestämmelserna om dataintrång och missbruk av urkund vem som har tilldelats ett eget utrymme.

   c. På samma sätt kan det för tillämpningen av regler om persondataskydd, t.ex. att en uppgift får lämnas elektroniskt till den registrerade själv, bli av betydelse vem som har tilldelats utrymmet.

[56] Se vidare eSams publikation Eget utrymme hos myndighet – en vägledning.
[57] Jfr hur pensionsinformation som samlats in och sammanställts av Min Pension i Sverige AB kan visas även på andra webbplatser än minpension.se, t.ex. efter inloggning på Pensionsmyndighetens eller ett försäkringsbolags webbplats.

7.3 Vidareförmedlingstjänster – sammansatta bastjänster

7.3.1 Utformning

1. Vidareförmedlingstjänster har beskrivits i avsnitt 6.5.1. Myndigheter inom eSam har utvecklat dessa så att de brukas även för presentationstjänster där uppgifter samlas in från flera källor till en användares eget utrymme och visas samlat och strukturerat för denne.

   Sådana funktioner tillhandahålls redan på Mina sidor inom Verksamt.se och av myndigheter som utanför Verksamt.se anslutit sina e-tjänster till Infrastrukturen för vidareförmedling av grundläggande uppgifter om företag, i flera sammanhang kallad SSBTGU.

7.3.2 Juridiska aspekter

2. De krav som beskrivits i kap. 6 när vidareförmedlingstjänster ger stöd åt servicetjänster tillämpas på motsvarande sätt i eget utrymme för presentationstjänster.

7.4 Säkerhetsarrangemang

3. För att ge den enskilde ett tillräckligt skydd och för att möjligheter till myndighets omedelbara hämtning, egen hämtning och egen delning inte ska leda till att allt som görs tillgängligt för att samlas in blir allmän handling hos den som tillhandahåller presentationstjänsten bör myndigheten närmare överväga vilka tekniska avgränsningar och skyddsåtgärder som ska införas. Utlämnande bör inte ske genom direktåtkomst.

7.4.1 Av straffrättslig betydelse och av betydelse för ansvarsfördelningen

1. Här behövs motsvarande arrangemang som i avsnitt 6.6.1 och 6.6.2.

7.4.2 Grundläggande arrangemang för informationssäkerheten

Se kap. 5.

7.5 Arkitekturer för presentationstjänst

1. Genom en presentationstjänst ges användaren av tjänsten möjlighet att få en överblick över information som kan ha hämtats både från myndighetens egna uppgiftssamlingar och från ett eller flera andra organ. När handlingar samlats in kan de – beroende på tjänstens utformning – bli allmänna även hos den myndighet som tillhandahåller presentationstjänsten.

2. Det som visas för en användare av en presentationstjänst avses dock inte bli tillgängligt för andra än användaren; jfr egen hämtning följd av visning i ett eget utrymme.

3. Särskilda åtgärder bör vidtas för att det som sammanställs och visas inte ska bli tillgängligt för annan än användaren.

7.5.1 Sättet för att hämta in underlag

4. Till en presentationstjänst hör arkitekturer för att, efter en visningsbegäran ta fram underlag från den egna myndigheten eller hämta in underlag från ett eller flera andra organ, genom

    a. myndighets omedelbara hämtning, från de organ som har underlaget, eller

    b. insamling på förhand, till

        i) den myndighet som tillhandahåller presentationstjänsten, eller,

        ii) en annan myndighet som endast har i uppgift att tekniskt lagra materialet, så att det omedelbart och i aktuell del kan lämnas ut till den myndighet som tillhandahåller presentationstjänsten, när visning begärs av visst material.

5. Som alternativ till en presentationstjänst kan visning ske med hjälp av bastjänster i en användares eget utrymme. Det sker genom egen hämtning följd av visning i eget utrymme. Skillnaden mellan den visning som sker i en servicetjänst respektive i en presentationstjänst är framförallt ändamålet. Uppgifterna ska visas för att informera användaren i presentationstjänsten medan syftet med att visa uppgifterna i servicetjänsten normalt är att användaren ska kunna utforma en ansökan eller liknande handling.

7.5.2 Med eller utan förhandsregistrering av användaren

6. En presentationstjänst där uppgifter hämtas, sammanställs och presenteras kan

    a. fungera utan registrering på förhand, genom att den enskilde vid varje visningstillfälle, efter legitimering, får lämna samtycke till användarvillkor och behandling av personuppgifter, eller

    b. förutsätta att den enskilde har registrerat sig.

7. De uppgifter som samlats in och sammanställts automatiserat bör hanteras så att åtkomst till materialet är utesluten för myndighetens personal, med undantag för åtkomst som är nödvändig för att åtgärda tekniska fel eller skydda mot angrepp eller annat missbruk.

En insamlad eller från detta underlag sammanställd eller bearbetad uppgift hos myndigheten bör gallras så snart det kan ske, om inte annat överenskommits med användaren och tillräckliga åtgärder har vidtagits för att skydda uppgifterna från oavsiktlig insyn och missbruk.

8. Hjälptjänster

8.1 Generella funktioner

1. Regeringen har förklarat att det i takt med att enskilda i allt högre grad använder digitala tjänster i kontakter med myndigheterna ställs högre krav på att erbjuda stöd och hjälp via internet (prop. 2016/17:198 s. 8). Genom hjälptjänster[58] – s.k. helpdesk – ger myndigheter användare stöd, så att

   a. tekniska fel eller fel vid användning av tjänster kan övervinnas, eller

   b. kompletterande information kan lämnas muntligen eller skriftligen till användare när viss information saknas eller användare inte förstår den information som lämnas elektroniskt.

2. Hjälptjänster kan utformas på olika sätt. Kommunikation sker i många fall muntligt, t. ex. per telefon, eller skriftligt via bl.a. chatt, sms, e-post eller vanlig post. Den hjälpsökande kan också vara uppkopplad mot t.ex. en presentationstjänst eller en servicetjänst. En utveckling pågår för att komplettera sådana tjänster med hjälptjänster, dvs. tjänster för att ge stöd till användare eller att förklara uppgifter som lämnas till användare där det som skriftligen kommer till myndigheten blir allmän handling.[59]

3. Till de mera avancerade funktioner som förekommer i hjälptjänster hör bl.a. att

   a. den som ger hjälp ska kunna

      i. se det som presenteras på den hjälpsökandes bildskärm, och

      ii. assistera i servicetjänsten för att korrigera felgrepp eller visa rätt användningssätt,

   b. den hjälpsökande ska få handlingar med stödjande information elektroniskt via hjälptjänsten.

4. Det som kommuniceras med en användare, för att tekniskt krångel eller andra svårigheter att förstå eller hantera uppgifter ska avhjälpas, avses inte bli tillgängligt för andra än den hjälpsökande och för den som ger hjälp. Därför bör hjälptjänster förenas med funktioner för omedelbar gallring.

5. De hjälptjänster som myndigheter tillhandahåller kan förenklat beskrivas utifrån följande varianter.

   a. Hjälpsökande och myndighet kommunicerare endast muntligt (med användaren inloggad).

   b. Utrymmesinnehavaren lämnar ut en skärmdump från sitt eget utrymme till hjälpfunktionen. Bilden blir allmän handling hos myndigheten men informationen i utrymmet skyddas alltjämt. Bilden bör så snart supportärendet är slutfört tas bort, förutsatt att det finns ett gallringsbeslut.

---

[58] Begreppet används här i en vidare mening än i E-delegationens betänkande Så enkelt som möjligt för så många som möjligt – Bättre juridiska förutsättningar förr samverkan och service (SOU 2014:39), där endast service genom en hjälptjänst för elektroniskt förvar (dvs. eget utrymme) innefattas.

[59] Regeringen har i lagmotiv anfört följande rörande hjälptjänster. ”En myndighets tillhandahållande av hjälptjänster till enskilda har en annan karaktär än den digitala tjänst som hjälptjänsten avser. De handlingar som kan uppstå i samband med tillhandahållandet av en hjälptjänst förvaras inte endast som led i teknisk bearbetning eller teknisk lagring för annans räkning. Även om tillhandahållandet av en hjälptjänst kan innefatta moment av teknisk bearbetning eller lagring kan det inte enbart anses utgöra sådan verksamhet” (prop. 2016/17:198 s. 24).

c. Utrymmesinnehavaren lämnar all nyttoinformation i eget utrymme till myndighetens hjälpfunktion. Därefter kan supportärendet genomföras elektroniskt i samverkan mellan användaren och befattningshavaren i hjälptjänsten. Utrymmet avslutas därmed. Materialet blir allmän handling.

d. Eventuellt kan därefter ett nytt eget utrymme skapas för användaren eller ett företag som denne agerar för. Den nyttoinformation som blivit allmän handling gallras så snart supportärendet har slutförts, förutsatt att det finns ett gallringsbeslut.

8.2 It-arkitekturernas funktionalitet

1. It-arkitekturen för en hjälptjänst bygger vanligtvis på att det finns
   a. en del för att samtala muntligt,
   b. en del för att se – och i vissa fall styra – den hjälpsökandes informationsbehandling,
   c. en kommunikationsdel där den som ger hjälp kan få meddelanden eller få till stånd åtkomst mellan berörda it-system,
   d. en del för omedelbar gallring, och
   e. viss funktionalitet för att skydda mot olovlig insyn eller vilseledanden varigenom att någon under sken av att vara en viss hjälpsökande eller verksam vid en viss hjälptjänst olovligen får del av eller annars kan använda uppgifter.

2. När uppgifter lämnas ut till en hjälpsökande utan att myndigheten och den hjälpsökande interagerar i realtid bör it-arkitekturen för hjälptjänsten utformas så att uppgifterna lämnas till ett eget utrymme som tillhandahålls åt den hjälpsökande.

8.3 Juridisk utformning

1. När uppgifter lämnas eller görs åtkomliga i en hjälptjänst aktualiseras frågor om allmänna handlingar, sekretess och persondataskydd. Förvaltningsrättsliga frågor kan också uppkomma. De handlingar som uppstår i samband med tillhandahållandet av en hjälpfunktion förvaras inte endast som led i teknisk bearbetning eller teknisk lagring för annans räkning. Även om tillhandahållandet av en hjälptjänst kan innefatta moment av teknisk bearbetning eller lagring kan det inte enbart anses utgöra sådan verksamhet (prop. 2016/17:198 s. 24).

2. Genom att ge befattningshavare vid en hjälpfunktion möjlighet att se det som den hjälpsökande har på sin skärm eller att assistera i servicetjänsten – och därigenom välja vad som syns – blir de handlingar som befattningshavaren på så sätt kan bereda sig tillgång till i läsbar eller annars uppfattbar form att anse som allmän handling hos den myndighet som ger hjälpen, så länge denna åtkomstmöjlighet består eller sådant material bevaras hos myndigheten. Den myndighet som ger hjälpen bör sträva efter lösningar där så litet material som möjligt görs tillgängligt så att det blir allmän handling.

3. På motsvarande sätt blir uppgifter hos en annan aktör, som görs tillgängliga via nät eller hämtas in till en myndighet för att myndighetens ska kunna lämna information, att anse som allmän handling där.

4. Information som hämtas in eller lämnas muntligt utgör dock inte ”handling” i tryckfrihetsförordningens mening. Spelas samtal in av en myndighet blir upptagningen emellertid allmän handling.

5. Hjälptjänster bör visserligen utformas så att den som ger hjälp och användaren av hjälptjänsten genast kan få relevant teknisk information eller annan information som krävs för att ge hjälpen. Några nya samlingar av allmänna handlingar bör emellertid inte byggas upp endast för att kunna ge hjälp.

6. En myndighet får 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) gallra handlingar som är av tillfällig eller ringa betydelse för myndighetens verksamhet, under förutsättning att allmänhetens rätt till insyn inte åsidosätts och att handlingarna bedöms sakna värde för rättskipning, förvaltning och forskning. De uppgifter som tillgängliggörs för myndighetens befattningshavare i samband med en hjälptjänst torde normalt endast vara av betydelse för myndighetens verksamhet under tiden som samtalet eller sessionen pågår. De handlingar som kan uppstå i samband med detta bör därmed oftast kunna gallras. Myndigheten behöver emellertid ha fattat ett gallringsbeslut som omfattar den aktuella informationen.

7. Sammantaget blir därmed möjligheterna att, med åberopande av reglerna om handlingsoffentlighet, få tillgång till uppgifter som har getts in eller gjorts tillgängliga vid användningen av en hjälptjänst ytterst begränsade (prop. 2016/17:198 s. 24). Någon allmän regel om tystnadsplikt finns emellertid inte för personal i en myndighets hjälptjänst.

8.4 Säkerhetsarrangemang

8. En hjälptjänst får inte utformas så att den leder till kartläggning av enskildas personliga förhållanden eller andra oönskade intrång i enskildas personliga integritet eller i uppgifter hos enskilda som de behöver hålla hemliga. Därför bör material gallras eller rensas bort så snart en hjälpsession för en användare som inte har ett konto är över. Bygger hjälptjänsten på konto bör bevarandefrågan klargöras i villkoren.

9. I övrigt behövs motsvarande arrangemang för informationssäkerheten som i avsnitt 6.6 och 7.4. Området utvecklas emellertid snabbt och de tekniska hjälpmedlen på marknaden är inte alltid anpassade för att kunna tillgodose de regler om offentlighet och sekretess och de särskilda behov av insynsskydd som finns på myndighetsområdet.

10. ”Som Integritetskommittén framhållit kan digitalisering av förvaltningen leda till ökade risker för den personliga integriteten och det är viktigt att myndigheter utformar sina digitala tjänster på ett sätt som minimerar dessa risker (SOU 2016:41). Myndigheter som tillhandahåller hjälptjänster bör därför vidta åtgärder som hindrar myndighetens personal och andra att missbruka information, t.ex. genom behörighetsstyrning, säkerhetsloggar och tekniska skyddsåtgärder” (prop. 2016/17:198 s. 25).

9. Kommentar

9.1 Ingen fullständig juridisk genomgång

Vissa förutsättningar är självklara från juridiska utgångspunkter, t.ex. att en myndighet inte får lagra fler uppgifter om enskilda än vad som krävs för att myndigheten ska kunna utföra sitt uppdrag. Vidare får en myndighet inte bereda sig tillgång till en enskilds eget utrymme eller använda sig av personuppgifter för ändamål som är oförenliga med dem för vilka uppgifterna samlades in, t.ex. för kartläggning eller övervakning av enskildas personliga förhållanden.[60]

Det skulle av utrymmesskäl föra för långt att i denna vägledning ha ambitionen att åstadkomma en heltäckande beskrivning av alla juridiska förutsättningar. I det följande begränsas genomgången till de särskilda konsekvenser som verksamhetsutveckling genom e-förvaltning kan föra med sig från juridiska utgångspunkter och hur en myndighet genom rätt utformade it-arkitekturer och rättsfigurer kan undanröja eller i vart fall minska risker från bl.a. rättssäkerhets-, informationssäkerhets-, och persondataskyddssynpunkt. Begränsningen kan innebära att läsaren behöver ha vissa juridiska grundkunskaper för att helt förstå resonemangen.

9.2 Inbyggt dataskydd och informationssäkerhet

> **Sammanfattning:** It-baserade tjänster för e-förvaltning bör ges sådan teknisk utformning att de ger skydd för den enskildes personliga integritet (s.k. inbyggt dataskydd eller privacy by design). Ett tillräckligt skydd för informationssäkerheten behöver också integreras med de it-miljöer där dessa it-baserade tjänster införs och förvaltas.

Inbyggda mekanismer för dataskydd tar sikte på bl.a. att uppgifter om

1. ett stort antal individer, så långt möjligt, inte ska behandlas på ett enda ställe, och
2. behandlingar i it-baserade tjänster inte ska finnas kvar där om det inte krävs, utan bevaras endast hos den som har behov av uppgifterna (se artikel 25 dataskyddsförordningen).

Sådana åtgärder för att bygga in ett dataskydd i it-arkitekturen kan bestå i att bl.a.

a. ha en vid krets av leverantörer av tjänster så att antalet uppgifter om enskilda kan begränsas hos respektive leverantör,

b. vidta åtgärder så att loggar och andra registreringar av personuppgifter inte innehåller onödiga uppgifter eller bevaras längre än nödvändigt,

c. aktivt utforma de tekniska lösningarna så att elektroniska spår inte uppstår annat än när det är nödvändigt,

d. överföra uppgifter som behövs i t.ex. bevissyfte till den som har behov av uppgifterna i stället för att bevara dem där de först uppkom,

e. använda funktioner för formulärdata så att endast viss användning tillåts,

[60] Se 2 kap. 6 § andra stycket regeringsformen (RF); jfr de begränsningar som får göras enligt 20 och 21 §§ samma kapitel. Genom krav på att myndighet inte får bereda sig tillgång till en enskilds eget utrymme eller dator m.m. undviks risken för sådana ”betydande intrång” i den personliga integriteten, som avses i 2 kap. 6 § andra stycket RF.

f. placera aktörernas funktioner och förvar så att behoven av bevis, för centrala frågor som avsändande, inkommande och ansvarsgränser i övrigt, inte i onödan inrymmer loggar, identitetsintyg, stämplar eller underskrifter eller leder till att svagare part får stå en risk när detta inte är sakligt motiverat.

De hot och risker som kan uppkomma för informationssäkerheten måste också beaktas så att alla berörda aktörer genomför ett systematiskt arbete för en tillräckligt hög skyddsnivå. Samordnade informationssäkerhetsskyddande funktioner behöver byggas in i berörda it-miljöer och stödjas av regelverk, som införs genom avtal, överenskommelser eller föreskrifter om vissa gemensamma skyddsnivåer, så att detta skydd säkerställs över tid.

9.3 Att särskilt beakta

Sammanfattning: En myndighet som tillhandahåller en elektronisk miljö åt enskilda måste beakta användarnas befogade förväntningar på att uppgifterna ska skyddas från bl.a. offentlighets- och informationssäkerhetssynpunkt och att frågor om fördelning av ansvar ska vara lösta. Detta gäller även när en myndighet använder en underleverantör. Skydd kan också ges genom regler om sekretess eller genom gallring eller rensning.

Utöver beskrivna utgångspunkter och arkitektoniska möjligheter att begränsa oönskade konsekvenser behöver vissa typfall uppmärksammas där it-baserade tjänster kan vara svåra att förena med gällande rätt. Dessa typfall rör bl.a. det stadium i den enskildes hantering av uppgifter där han eller hon inte har gett in någon handling i ett ärende utan ges tekniskt och administrativt stöd för att kunna upprätta och skriva under handlingar och ge in dem i ett serviceskede med stöd av ett eget utrymme.[61]

Det är när uppgifter ska behandlas i ett sådant utrymme som konsekvenser från juridiska utgångspunkter framträder särskilt tydligt. Den enskilde har en befogad förväntan på att uppgifterna ska vara skyddade från både offentlighets- och sekretessynpunkt och från persondataskydds- och informationssäkerhetssynpunkt. Författningsregleringen har dock i huvudsak utformats när myndigheter inte elektroniskt tillhandahöll egna utrymmen eller annat stöd åt enskilda för att kunna upprätta, ge in och motta uppgifter och handlingar.

De rättsliga konsekvenser som kan uppkomma vid felaktiga val av it-arkitekturer eller rättsfigurer beskrivs i det följande. Här bör emellertid erinras om att en myndighets ansvar beträffande handlingsoffentlighet, sekretess samt bevarande och gallring naturligtvis gäller även när myndigheten använder sig av en tjänst för teknisk bearbetning och teknisk lagring som en underleverantör ställer till myndighetens förfogande (extern it-drift).

Myndigheten har ett ansvar för att säkerställa informationshanteringen inte bara från ett konfidentialitetsperspektiv, utan även med avseende på informationens riktighet, tillgänglighet, spårbarhet och äkthet. Vem som är informationsägare bör därför vara tydligt uttryckt och godtaget av alla parter i de olika faserna av informationshanteringen. Med detta följer också att informationsägaren tydligt ska informera enskilda vad de kan förvänta sig för skyddsnivå utifrån dessa olika

Myndigheten har ett ansvar för att säkerställa informationshanteringen inte bara från ett konfidentialitetsperspektiv, utan även med avseende på informationens riktighet, tillgänglighet, spårbarhet och äkthet.

[61] Samtidigt pågår en snabb utveckling mot att enskilda elektroniskt ska kunna motta och besvara förelägganden och andra handlingar, under det skede där myndigheten handlägger ärendet, och att enskilda även i övrigt ska kunna använda säker elektronisk post, bl.a. för att motta myndighetsbeslut.

aspekter. Samtidigt får denna information inte avslöja uppgifter som är känsliga från säkerhetssynpunkt (jfr 18 kap. 8 § OSL).

9.4 Handlingsoffentlighet

Sammanfattning: Reglerna om handlingsoffentlighet innebär i korthet att alla uppgifter som en myndighet har tillgång till med sina tekniska hjälpmedel blir allmänna handlingar hos myndigheten och kan begäras ut enligt offentlighetsprincipen om de inte omfattas av sekretess. Det finns emellertid undantag, bl.a. ett för handling som förvaras hos en myndighet endast som led i teknisk bearbetning eller teknisk lagring för annans räkning. Med rätt utformade it-arkitekturer och skydd för uppgifter från åtkomst av myndighetens handläggare och tekniker kan en it-baserad tjänst i många fall tillgodose enskildas befogade förväntningar på att uppgifter inte ska bli tillgängliga för annan.

Regleringen

Reglerna om handlingsoffentlighet och sekretess har delvis utformats utan anpassning till elektronisk kommunikation och it-baserade tjänster. För e-förvaltningen är det en särskild utmaning att en handling[62] anses vara både förvarad och inkommen (och därmed allmän så att handlingen kan begäras ut av var och en om den inte innehåller sekretessbelagda uppgifter) redan när annan har gjort den tillgänglig för myndighet med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att handlingen kan läsas eller på annat sätt uppfattas.[63]

Utformas it-arkitekturen så att en myndighet hos någon annan (myndighet eller företag) kan komma åt uppgifter eller handlingar blir dessa normalt allmänna handlingar hos den myndighet som ges tillgång till materialet. Detta gäller även om den myndighet som kan komma åt handlingar aldrig har för avsikt att använda och inte heller behöver komma åt någon av handlingarna.

Det kan till och med vara så att myndigheten inte ska ha tillgång till en handling men att sådan åtkomst råkat uppkomma. Även i ett sådant fall blir handlingen allmän och därtill offentlig hos den myndighet som ges åtkomst, om handlingen inte är sekretessbelagd. Till detta kommer att en rättslig begränsning av ändamålet – så att en utlämnande myndighet enligt lag eller förordning inte får ta del av eller annars använda en tekniskt tillgänglig handling – i många fall inte gäller när en handling begärs utlämnad med stöd av offentlighetsprincipen eftersom grundlag gäller framför en rättslig begränsning som inte är förenlig med grundlag. Det uppkommer därför ett ”överskott av allmänna handlingar”.[64] Uppgifter blir normalt tekniskt tillgängliga för en myndighet som

1. tillhandahåller egna utrymmen (för en session eller som konto eller brevlåda), eller
2. ges tillgång till uppgifter hos någon annan, myndighet eller enskild, för att kunna ta fram uppgifterna när de behövs, t.ex. i en presentationstjänst.

Enligt regeringens uppfattning är det dock rimligt att enskilda ska kunna förvänta sig att uppgifter som de lämnar i eget utrymme skyddas såväl mot insyn från allmänheten som mot obehörigt utnyttjande från dem som har teknisk tillgång till uppgifterna (prop. 2016/17:198 s. 17).

[62] Begreppet är så vidsträckt att det innefattar inte bara färdiga handlingar utan i princip alla sammanställningar av uppgifter som myndigheten kan göra tillgängliga med rutinbetonade åtgärder.
[63] För sammanställningar gäller visserligen en begränsning till vad som är rutinbetonat men detta rekvisit inrymmer betydande åtgärder för att skapa nya uppgiftskonstellationer.
[64] Se vidare Informationshanteringsutredningens betänkande Överskottsinformation vid direktåtkomst (SOU 2012:90).

Centrala undantag från offentlighetsinsyn

Det finns två paragrafer av särskild praktisk betydelse i myndigheternas it-verksamhet där det föreskrivs att vissa handlingar inte är allmänna. Som allmän handling anses inte

- handling som förvaras hos en myndighet endast som led i teknisk bearbetning eller teknisk lagring för annans räkning (10 § första stycket), och
- brev, telegram eller annan sådan handling som har inlämnats till eller upprättats hos myndighet endast för befordran av meddelande (11 §).

Undantaget för befordran av meddelanden har lagts till grund för den elektroniska förmedlingsfunktion som Tillväxtverket tillhandahåller enligt 7 § förordningen (2009:1078) om tjänster på den inre marknaden (se paragrafens andra stycke). Tjänster och funktioner för e-förvaltning bygger även i övrigt till betydande del på en tillämpning av undantaget för endast teknisk bearbetning eller teknisk lagring för annans räkning (2 kap. 10 första stycket § TF) och att ingen annan än innehavaren ska få ha insyn i nyttoinformation i eget utrymme.[65]

Om it-arkitekturen och de ändamål för vilka den används utformas felaktigt, och om uppgifterna inte är sekretessbelagda, kan konsekvensen dock bli att uppgifter och handlingar som enskilda ser som sina egna, utan att andra ska ha rätt att ta del av dem, blir allmänna och offentliga handlingar. Vid tillämpningen av rekvisitet ”endast” som ett led i teknisk bearbetning eller teknisk lagring för annans räkning, enligt 2 kap. 10 § TF, bör det särskilt beaktas att det är av avgörande betydelse att en myndighet som tillhandahåller sådan service inte samtidigt använder uppgifterna för sin egen verksamhet.

Att särskilt observera: En myndighet som tillhandahåller en funktion som bygger på något av dessa undantag bör vidta särskilda åtgärder för att säkerställa att handlingarna inte finns tillgängliga vid myndigheten för annat ändamål än vad som anges i berörd undantagsbestämmelse; dvs. att de används endast för teknisk bearbetning eller teknisk lagring för annans räkning respektive brukas endast för befordran av meddelande.

Utlämnande som inte leder till tillgänglighet enligt 2 kap. tryckfrihetsförordningen

Begreppen direktåtkomst och utlämnande på medium för automatiserad behandling förekommer inte i 2 kap. TF. Vid direktåtkomst uppkommer dock, så som dagens it-arkitekturer är utformade, ofta överskottsinformation i form av allmänna handlingar hos mottagande myndighet redan till följd av att handlingar blir tillgängliga.

När informationssystem kommunicerar i realtid och befattningshavare får svar genast, även över organisationsgränser, har det i vissa fall blivit delvis oklart vilken prövning som görs, vem som gör prövningen, vilka beslut som fattas i olika led av hanteringen och vem som ansvarar för respektive led. Situationen har ytterligare komplicerats av att myndigheternas it-baserade tjänster ofta förutsätter tillgång till fler uppgifter om en person eller uppgifter om fler personer än vad myndigheten behöver för sin ärendehandläggning.

[65] Se vidare prop. 2016/17:198 och eSams rättsliga uttalande den 22 november 2017 Eget utrymme hos myndighet och en promemoria den 22 november 2017 Eget utrymme är numera accepterat i lagmotiv.

Rättsläget har delvis klarlagts genom att det i rättspraxis prövats vad som menas med direktåtkomst. Denna tolkning har samordnats med när en handling anses vara tillgänglig för en myndighet enligt 2 kap. 3 § andra stycket TF (se vidare HFD 2015 ref. 6 och den redovisning som ges i avsnitt 2.7). Myndigheter bör utforma sitt informationsutbyte så att direktåtkomst inte uppkommer. På samma sätt bör egen hämtning och egen delning inte ske genom direktåtkomst. När en myndighet eller ett annat organ, istället för att på förhand ge direktåtkomst till handlingar, på begäran i varje enskilt fall beslutar om en handling ska lämnas ut, blir de handlingar som förvaras hos det utlämnande organet inte tekniskt tillgängliga på förhand för den begärande myndigheten. Istället för direktåtkomst blir det därmed fråga om s.k. utlämnande på medium för automatiserad behandling. Utformas it-arkitekturen rätt blir handlingar vid ett sådant utlämnande inte att anse som allmänna på förhand hos en begärande myndighet utan först efter att de aktivt lämnats ut.

Att särskilt observera: En myndighet som överväger att införa en it-baserad tjänst där informationsutbyte ingår bör utforma funktionerna så att överskottsinformation inte uppkommer.

9.5 Sekretess och tystnadsplikt

I offentlighets- och sekretesslagen (2009:400; OSL) finns bestämmelser om förbud mot att lämna ut handlingar och om tystnadsplikt för befattningshavare. Enligt dessa bestämmelser får sekretessbelagda uppgifter inte röjas, vare sig muntligen, genom utlämnande av allmän handling eller på något annat sätt, se vidare t.ex. den närmare redovisningen av gällande rätt i regeringens proposition 2016/17:198 Utökat sekretesskydd i verksamhet för teknisk bearbetning och lagring.

En för den enskilde självklar förutsättning vid användningen av ett eget utrymme är att det material som finns där varken lämnas ut eller annars röjs; jfr om ett utkast till en ännu inte färdigställd årsredovisning för ett börsbolag, som togs fram i Bolagsverkets ärendetjänst för årsredovisning, hade lämnats ut som allmän och offentlig handling eller om en befattningshavare hade röjt detta materials innehåll innan det färdigställts och getts in.

Material i ett eget utrymme lämnas inte ut som allmän handling om det förvaras av en myndighet endast som led i teknisk bearbetning eller teknisk lagring för annans räkning. Det kan emellertid också behövas ett skydd för material som blir tillgängligt för den som arbetar med utveckling och drift av egna utrymmen så att han eller hon inte får röja uppgifter som finns i ett sådant utrymme. I verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning gäller också en bestämmelse om förbud mot att lämna ut handlingar och om tystnadsplikt för befattningshavare (40 kap. 5 § OSL). Skyddet gäller visserligen bara för uppgift om en enskilds personliga eller ekonomiska förhållanden men det är från år 2018 inte längre begränsat till personuppgifter – även t.ex. företagsuppgifter skyddas (se prop. 2016/17:198).

Att särskilt observera: En myndighet som tillhandahåller eget utrymme åt enskilda bör införa sådana tydliga förbud för befattningshavare mot att ta del av eller annars använda innehållet i enskilds eget utrymme att den som bryter mot förbudet gör sig skyldig till dataintrång.

9.6 Sekretessbrytande bestämmelser

Sekretess gäller som huvudregel inte bara i förhållande till enskilda utan också mellan myndigheter samt inom en myndighet, om där finns olika verksamhetsgrenar som är att betrakta som självständiga i förhållande till varandra (8 kap. 1 och 2 §§ OSL). I vissa fall måste dock myndigheter kunna utbyta sekretessbelagda uppgifter för att utföra sina uppgifter. Sekretessregleringen innehåller därför sekretessbrytande bestämmelser som innebär att en sekretessbelagd uppgift får lämnas ut under vissa förutsättningar. En sekretessbrytande bestämmelse möjliggör alltså ett utbyte av uppgifter mellan myndigheter utan hinder av att uppgifterna är sekretessreglerade.[66]

En myndighet som överväger att införa en it-baserad tjänst där informationsutbyte ingår bör, förutom att förvissa sig om att informationsutbytet i sig är tillåtet, granska om den planerade tjänsten innefattar ett utlämnande av uppgifter som är sekretessreglerade och därmed kan komma att vara sekretessbelagda i enskilda fall samt om uppgifterna röjs. Myndigheten bör i så fall granska om ett sådant utlämnande omfattas av en sekretessbrytande regel.

9.7 Överföring av sekretess

Om en sekretessreglerad uppgift lämnas från en myndighet till en annan gäller sekretess för uppgiften hos den mottagande myndigheten antingen om sekretess följer av en primär sekretessbestämmelse, som är tillämplig hos den mottagande myndigheten, eller om sekretess följer av en bestämmelse om överföring av sekretess. Om ingen av dessa förutsättningar är uppfyllda blir uppgiften offentlig hos den mottagande myndigheten (7 kap. 2 § OSL).

Om direktåtkomst ges till uppgifter eller handlingar, så att de därigenom blir allmänna handlingar hos den myndighet som ges åtkomst, kan sekretessen komma att överföras (se 11 kap. 4 § OSL). En bestämmelse har dessutom från år 2018 införts om att sekretessen vid endast teknisk bearbetning och lagring för en annan myndighets räkning överförs, om en myndighet i sådan verksamhet får en uppgift som är sekretessreglerad av hänsyn till ett allmänt intresse (11 kap. 4 a § OSL och prop. 2016/17:198).

Att särskilt observera: Har en myndighet hos en annan myndighet elektronisk tillgång till en upptagning för automatiserad behandling och en uppgift i denna är sekretessreglerad blir sekretessen normalt tillämplig även hos den mottagande myndigheten. Får en myndighet i verksamhet för enbart teknisk bearbetning och lagring för annan myndighets räkning uppgifter som är sekretessreglerade där av hänsyn till ett allmänt intresse blir bestämmelsen tillämplig även hos den mottagande myndigheten.

[66] Se 3 kap. 1 § OSL för definitioner samt Justitiedepartementets informationsskrift Offentlighetsprincipen och sekretess, http://www.regeringen.se/sb/d/108/a/208071.

9.8 Bevarande och gallring

Sammanfattning: För att tillgodose enskildas befogade förväntningar på att andra inte ska kunna ges tillgång till information som den enskilde ser som sin egen och att enskild inte ska kunna spåras eller övervakas utifrån tjänstens användning kan beslut om omedelbar gallring behöva fattas så att uppgifter som har blivit allmän handling får

1. tas bort genast efter att de har presenterats för en enskild respektive brukats för att ge den enskilde hjälp och stöd, eller
2. göras oåtkomliga för myndigheten, så snart den enskilde inte längre behöver dem.

Reglerna om bevarande och gallring – som ska tillämpas beträffande allmänna handlingar, bl.a. när ovan nämnda bestämmelse i 2 kap. 10 § TF inte blir aktuell – förutsätter att myndigheterna intar ett aktivt förhållningssätt till sin informationshantering.[67] Konsekvenser som inte är önskade kan uppkomma om uppgifter som blivit allmän handling finns kvar och kan begäras ut av var och en samtidigt som de saknar betydelse för myndighetens verksamhet och inte längre behöver användas av en enskild.

En myndighet som ska tillhandahålla en it-baserad tjänst behöver redan när tjänsten utvecklas se till att frågor om bevarande, gallring och rensning blir lösta så att en god offentlighetsstruktur kan upprätthållas och att oönskade konsekvenser inte uppkommer för enskilda.

Arkivförfattningarna blir tillämpliga redan när en handling har blivit allmän enligt 2 kap. TF. Dessutom är definitionen av handling (upptagning) så vid att teknisk information och de sammanställningar som en myndighet kan göra med rutinbetonade åtgärder av uppgifter i en it-baserad tjänst kan bli att anse som allmän handling och därmed som arkivhandling hos myndigheten. Både nyttoinformation och drift- och säkerhetsrelaterad information kan komma att bevaras i en omfattning som enskilda inte väntar sig. Vissa it-baserade tjänster är dessutom utformade så att en myndighet hos sig samlar in eller har åtkomst till handlingar endast för att erbjuda t.ex. en presentationstjänst.

Statliga myndigheter får enligt 14 § arkivförordningen (1991:446) gallra allmänna handlingar endast i enlighet med föreskrifter eller beslut av Riksarkivet. För kommunala myndigheter föreskriver respektive kommun- eller landstingsfullmäktige om hur arkivlagens bestämmelser ska tillämpas för dem. Frågan om gallringsbeslut behöver alltså lösas redan innan en it-baserad tjänst tas i drift. Behöver material som inte blivit allmän handling tas bort – s.k. rensning – krävs dock inte sådant beslut.

För handlingar som har blivit allmänna men som är av tillfällig eller ringa betydelse har Riksarkivet föreskrivit att de får gallras under förutsättning att allmänhetens rätt till insyn inte åsidosätts och handlingarna bedöms sakna värde för rättsskipning, förvaltning och forskning. Sådan gallring ska ske vid en tidpunkt eller efter en frist som fastställts av myndigheten (RA-FS 1991:6, ändrad 1997:6). Vid denna bedömning måste myndigheten uppmärksamma att en rad olika åtgärder kan bli att anse som gallring, t.ex. om myndigheten överför uppgifter så att detta medför:

[67] Enligt 3 § arkivlagen (1990:782) ska allmänna handlingar 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 (3 §). Men allmänna handlingar får gallras endast under förutsättning att föreskrivna bevarandemål kan tillgodoses (10 §).

– informationsförlust

– förlust av möjliga informationssammanställningar,

– förlust av sökmöjligheter, eller

– förlust av möjligheter att fastställa informationens autenticitet.[68]

Beträffande allmänna handlingar som är av tillfällig eller ringa betydelse får en myndighet själv fatta beslut om gallring, jfr prop. 2016/17:198 s. 24 där regeringen uttalat att de uppgifter som tillgängliggörs för en myndighets befattningshavare i samband med en hjälptjänst normalt torde vara endast av betydelse för myndighetens verksamhet under tiden som samtalet eller sessionen pågår och att de handlingar som kan uppstå i samband med detta därmed oftast bör kunna gallras, se vidare Riksarkivets råd och vägledningar som finns tillgängliga på https://riksarkivet.se/vardera-och-gallra. Myndigheten får själv bestämma om rensning av data som inte utgör allmän handling.

Att särskilt observera: Information som skapas i anknytning till it-baserade tjänster och som blivit allmänna handlingar kan vara av sådan tillfällig eller ringa betydelse att gallringsbeslut kan fattas av den myndighet som tillhandahåller den it-baserade tjänsten. Även partiella åtgärder, t.ex. förlust av möjlighet att fastställa autenticitet kan vara gallring som kräver beslut om åtgärden.

9.9 Förvaltningsrättsliga frågor om service och inkommande

Sammanfattning: En myndighet kan i ett ”serviceskede” tillhandahålla elektroniskt stöd och göra elektroniska kontroller innan en handling ges in till en elektronisk mottagningsfunktion.

Genom regeringens proposition 2016/17:180 En modern och rättssäker förvaltning – ny förvaltningslag, införs nya regler som träder i kraft den 1 juli 2018 (SFS 2017:900) om bl.a. service och inkommande handlingar. Inte heller genom denna reglering framstår emellertid den förvaltningsrättsliga regleringen som helt anpassad till it-baserade tjänster. Den som använder t.ex. en servicetjänst ges hjälp och stöd på ett sätt som liknar den hjälp som en handläggare ger vid ett personligt besök hos myndigheten. I it-miljön sker emellertid allt automatiserat i det skede – serviceskedet – när utkast till elektroniska handlingar skapas och annars hanteras i den enskildes eget utrymme.

Det är en förutsättning för att en servicetjänst ska fungera att material i den enskildes eget utrymme, t.ex. när en enskild tar fram ett utkast till en deklaration i en e-tjänst hos Skatteverket, inte anses inkommet enligt förvaltningslagen till den myndighet som tillhandahåller det egna utrymmet.[69] På samma sätt kan en handling inte anses ha kommit in till en myndighet för att den mellanlagras på ett konto för en enskild eller för att en enskild i ett eget utrymme granskar en färdig text inför underskrift.

En myndighet kan av sakligt motiverade administrativa skäl eller säkerhetsskäl i ett serviceskede i ett eget utrymme införa automatiserade kontroller för att ge enskilda stöd när handlingar skapas och därigenom undvika att handlingar ges

[68] För det statliga området har Riksarkivet meddelat föreskrifter och allmänna råd om bl.a. gallring och utlån av räkenskapshandlingar (RA-FS 2004:3), se även Riksarkivets rapport 2005:1, Bevarande av räkenskaper – kommentarer till RA-FS 2004:3.

[69] En myndighet har normalt flera kanaler för att ge in handlingar och flera mottagningsfunktioner, t.ex. för olika servicetjänster och för e-post. Samma rättssäkerhetsgarantier bör gälla för dessa kanaler.

in om det finns brister som upptäcks genom sådana kontroller. Kontroller av detta slag får inte – om servicetjänsten ska fungera – leda till att material anses inkommet. Materialet har i det skedet inte nått myndighetens mottagningsfunktion.

Enligt 22 § förvaltningslagen (2017:900) har en handling kommit in till en myndighet den dag som handlingen når myndigheten eller en behörig befattningshavare. För elektronisk ingivning i anknytning till e-tjänster blir handlingen i praktiken inkommen när den nått myndighetens funktion för mottagning av sådana försändelser. Eftersom (data som representerar) handlingen genast når myndighetens funktion för att ta emot sådana försändelser, och tidpunkten för inkommande registreras där, blir det enligt eSams rättsliga expertgrupps bedömning enkelt att i förvaltningsrättslig mening avgöra och bevisa när en handling har kommit in. I praktiken leder detta till samma inkommandetidpunkt som enligt den hjälpregel för it-miljö som Förvaltningslagsutredningen föreslagit och enligt vilken en handling som sänts till ett anvisat elektroniskt mottagningsställe, ska anses ha kommit in när den har tagits emot där.

Det är emellertid delvis höljt i dunkel hur de situationer ska bedömas när det uppstår något hinder eller fel vid överföringen. Dessa frågor redovisas närmare i eSams rättsliga uttalande den 26 oktober 2017 Ankomstdag för elektroniska handlingar och en promemoria den 31 oktober 2017 inkommandetidpunkt – när har en handling kommit in till myndighet?

Myndigheternas mottagningsfunktioner bör utformas så att kvittens sänds när en försändelse har nått myndighetens mottagningsfunktion och att felmeddelande lämnas om försändelsen helt eller delvis inte har kunnat läsas av myndigheten. Myndigheten bör löpande registrera händelser som kan tyda på fel i någon funktion där myndigheten tar emot inkommande handlingar.

9.10 Behandling av personuppgifter

Utgångspunkter

En avvägning mellan integritet och effektivitet måste alltid göras när en ny it-baserad tjänst planeras och det måste finnas en rättslig grund för alla behandlingar av personuppgifter.[70] Myndigheters uppgifter som har stöd i rättsordningen utgör sådana uppgifter av allmänt intresse som regleras av dataskyddsförordningen och som utgör rättslig grund för behandling av personuppgifter. Det medför att kravet på rättslig grund är uppfyllt då myndigheter inför it-baserade tjänster som ett led i utförande av sina instruktionsenliga uppgifter.[71] Att det finns en rättslig grund för behandlingen av personuppgifter är dock i sig inte tillräckligt för att personuppgiftsbehandlingen ska vara laglig, utan samtliga krav i dataskyddsförordningen och kompletterande lagstiftning måste beaktas.

Det kan vara så att särskilda registerförfattningar gäller för vissa av de behandlingar av personuppgifter som berörs av it-baserade tjänster. En myndighet som vill införa en sådan tjänst behöver därför kartlägga om någon registerförfattning kan bli tillämplig och – när så är fallet – hur denna reglering kan förenas med den planerade tjänsten. Bestämmelser som särskilt bör uppmärksammas inom ett område där en registerförfattning gäller är om ändamålsbegränsningar eller särskilda regler om utlämnande av uppgifter behöver ändras om tjänsten ska införas.

[70] Se vidare t.ex. Datainspektionens vägledningar om hur personuppgiftslagen ska tillämpas i anknytning till bl.a. it-baserade tjänster; www.datainspektionen.se.
[71] Se Dataskyddsutredningens betänkande Ny dataskyddslag Kompletterande bestämmelser till EU:s dataskyddsförordning (SOU 2017:39), s 122 ff.

För många frågor om persondataskydd finns närmast självklara lösningar när it-baserade tjänster ska införas. I andra delar kan särskilda komplikationer uppkomma; bl.a. rörande frågor om

1. stöd behövs i lag för att införa en viss tjänst till följd av behandlingarnas karaktär eller om författningsändringar krävs för att göra tjänsten förenlig med en registerförfattning,
2. hur personuppgiftsansvarets ska anses vara fördelat mellan aktörerna enligt dataskyddsförordningen eller en registerförfattning,
3. information till registrerade om behandlingar, samt
4. vilka risker som uppkommer från säkerhetssynpunkt.

Personuppgiftsansvaret

Sammanfattning: De aktörer som berörs av it-baserade tjänster och tillhörande kanaler för att nå egna utrymmen eller transportkanaler för att ge in handlingar behöver klargöra mellan sig vem eller vilka som har personuppgiftsansvaret för respektive del och vad ansvaret innebär i olika avseenden, bl.a. säkerhetsmässigt och när underleverantörer anlitas.

Personuppgiftsansvarig är den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter (artikel 4.7 dataskyddsförordningen). Det är den som är personuppgiftsansvarig för en behandling av personuppgifter som är skyldig att se till att de skyldigheter och rättigheter som dataskyddslagstiftningen föreskriver uppfylls.

De olika tjänster och kommunikationskanaler som införs för e-förvaltningen berör olika aktörer. Ett första steg för att ta ställning till vilket ansvar en myndighet har vid införande av en e-tjänst är därför att kartlägga vilka behandlingar av personuppgifter som kommer att äga rum, för att därefter göra en bedömning av vem som bestämmer ändamål och medel för respektive behandling.

Det kan också vara så att dataskyddsförordningen inte gäller för den enskildes egen behandling av personuppgifter i e-tjänsten, om den enskildes behandling omfattas av det så kallade hushållsundantaget i artikel 2.2 c) i dataskyddsförordningen. Även om hushållsundantaget är tillämpligt för den enskildes egen behandling måste tillhandahållaren av e-tjänsten fortfarande ta ställning till vilken behandling av personuppgifter som denne bestämmer ändamål och medel för, och därmed bär personuppgiftsansvaret för.

När ett meddelande har nått fram till en myndighets anvisade mottagningsfunktion blir den mottagande myndigheten normalt personuppgiftsansvarig.

Särskilda frågor om personuppgiftsansvar uppkommer vid elektronisk legitimering och elektronisk underskrift samt vid meddelandeförmedling. Personuppgiftsansvaret inom Infrastrukturen för Svensk e-legitimation flyttas stegvis, i takt med att en transaktion flödar genom den. På liknande sätt flyttas personuppgiftsansvaret stegvis inom Infrastrukturen för säkra elektroniska försändelser

(Mina meddelanden).[72] Inte heller i denna del har frågan om ansvarsfördelning varit föremål för prövning i domstol.

Biträdesavtal

Personuppgiftsansvariga kan anlita leverantörer av it-tjänster. De agerar vanligtvis i egenskap av personuppgiftsbiträde. De personer som arbetar under biträdets eller den personuppgiftsansvariges ledning får behandla personuppgifter endast i enlighet med instruktioner från den personuppgiftsansvarige. Ett skriftligt avtal med visst innehåll måste finnas om personuppgiftsbiträdets behandling av personuppgifter för den ansvariges räkning (artikel 28 dataskyddsförordningen).

Att särskilt observera: Glöm inte att ingå de biträdesavtal som krävs när en it-baserad tjänst införs.

Information

Sammanfattning: Den information som måste lämnas enligt lag är omfattande och bör samlas så att den blir enkel att ta del av.

Inom ramen för en it-baserad tjänst och den infrastruktur som den är ansluten till måste myndigheten lämna all information som krävs för att den enskilde ska kunna ta tillvara sina rättigheter i fråga om behandlingar som äger rum hos de olika aktörerna.

Informationen måste vara tydlig så att en enskild kan se och förstå vem som ansvarar för vad. Vem som är personuppgiftsansvarig ska således framgå för varje del av kedjan. Det bör också vara tydligt för enskilda vad de kan förvänta sig beträffande konfidentialitet, riktighet, tillgänglighet, spårbarhet och äkthet. Det kan ofta vara lämpligt att en aktör i sin tjänst tillhandahåller information om en hel kedja av behandlingar där olika personuppgiftsansvariga är inblandade, eller hänvisar till en sådan plats, så att den enskilde kan få en överblick över berörda personuppgiftsbehandlingar.[73] Informationen bör även omfatta i vilken utsträckning handlingar blir allmänna enligt 2 kap. TF och vilka rutiner som tagits fram beträffande bevarande, gallring och rensning. Detta är särskilt angeläget om behandlingen avviker från vad en enskild kan antas förvänta sig.

Skyddsåtgärder

Sammanfattning: Varje aktör är ansvarig för att vidta lämpliga tekniska och organisatoriska åtgärder för behandlingar som denne är personuppgiftsansvarig för och att vidta de åtgärder som krävs för att åstadkommer en lämplig säkerhetsnivå.[74]

---

[72] Anslutna aktörer har utgått från att Skatteverket är personuppgiftsansvarigt för de behandlingar som verket utför i samband med ansökning, anslutning och användning av förmedlingsadressregistret och avsändande myndighet är personuppgiftsansvarig för behandlingar i samband med upprättande och expediering av försändelser. Brevlådeoperatören är personuppgiftsansvarig för de behandlingar som sker för elektronisk postbefordran (mottagning, sortering och utdelning i e-brevlådor av försändelser) och för de behandlingar för kontroll som sker vid tillträde till en brevlåda. Brevlådeinnehavaren är ansvarig för nyttoinformationen i sitt eget utrymme (e-brevlådan). Operatören svarar för den drift- och säkerhetsrelaterade information som avser den enskildes eget utrymme och i övrigt för att de personuppgifter som behandlas i utrymmet är omgärdade av adekvata säkerhetsåtgärder. För innehållet i ett befordrat meddelande är dock den avsändande myndigheten personuppgiftsansvarig även under det skede när det är under befordran av en brevlådeoperatör; jfr punkten 47 i ingressen till Dataskyddsdirektivet.

[73] Jfr E-nämndens vägledning (05:04) för information som enligt lag ska lämnas på webbplatser.

[74] En samordning av myndigheternas arbete för informationssäkerhet sker emellertid genom bl.a. Myndigheten för samhällsskydd och beredskap (MSB).

Av avgörande betydelse för att kunna införa en it-baserad tjänst är att de säkerhetsrelaterade risker som följer av införandet analyseras och beaktas (artikel 32 dataskyddsförordningen). Den som är personuppgiftsansvarig för en behandling av personuppgifter måste därför vidta lämpliga tekniska och organisatoriska åtgärder för att skydda behandlade personuppgifter. Det innefattar även bedömningar och analyser av vad ansvaret innebär i olika avseenden, bl.a. när ett personuppgiftsbiträde anlitas. I detta sammanhang förtjänas åter att påpekas vikten av att informera enskilda, t.ex. om vilka rättigheter respektive skyldigheter myndigheten och den enskilde har när det gäller den information som behandlas och om vilket ansvar som myndigheten påtar sig, t.ex. för att informationen lagras på beständigt sätt och hur länge det sker.

Personuppgiftsansvariga organ behöver initialt och regelbundet utföra riskanalyser. En sådan analys behöver innefatta hela den serie av behandlingar för vilka en personuppgiftsansvarig har att svara (HFD 2012 ref. 21). Sådana analyser bör lämpligen utföras och åtgärder vidtas i samverkan mellan berörda aktörer så att ett enhetligt skydd kan upprätthållas inom ramen för de samordnade infrastrukturer för it-baserade tjänster som verksamhetsutvecklingen inom e-förvaltningen för med sig. Beroende på vilken risk en tilltänkt behandling av personuppgifter innebär för enskildas rättigheter och friheter kan den personuppgiftsansvarige behöva utföra en konsekvensbedömning avseende dataskydd innan behandlingen inleds (artikel 35 dataskyddsförordningen).

Aktörer som ansluts genom avtal bör civilrättsligt åläggas sådana skyldigheter att ett omedelbart och kraftfullt agerande blir möjligt när ett nytt hot eller en ny risk tillkommer. Aktörerna bör också genom avtal förpliktas att rapportera it-incidenter så att skyddsåtgärder kan samordnas.

Regler i registerförfattningar

Sammanfattning: En myndighet som planerar en it-baserad tjänst behöver undersöka om en eller flera registerförfattningar kan bli tillämpliga och analysera om de kan förenas med den hantering av uppgifter som planeras i anknytning till tjänsten.

För åtskilliga myndigheter och verksamheter finns särskilda s.k. registerförfattningar. Vissa sådana författningar anger för vilka ändamål uppgifter får behandlas. Blir en sådan ändamålsbegränsning tillämplig på behandlingar i en it-baserad tjänst måste den personuppgiftsansvarige kontrollera att de planerade behandlingarna kan förenas med föreskrivna ändamål. Faller de planerade behandlingarna inte inom denna ram krävs författningsändringar, om ändamålen är uttömmande angivna i den särskilda regleringen. Är de inte uttömmande angivna där får dock behandlingar som inte är oförenliga med angivna ändamål äga rum (se artikel 5.b i dataskyddsförordningen).

En annan central fråga vid elektroniskt informationsutbyte är om uppgifter får lämnas ut på elektronisk väg[75]. I den mån en registerlag inte reglerar frågan om elektroniskt utlämnande finns normalt inte hinder mot att lämna ut uppgifterna elektroniskt, om det kan ske på ett säkert sätt. Det krävs alltså inte något uttryckligt mandat i en författning för att expediering på elektronisk väg ska vara tillåten. Flera registerlagar anger emellertid att utlämnande på elektronisk

[75] En förutsättning är förstås att sekretess inte hindrar ett utlämnande.

väg får ske endast om det har föreskrivits av regeringen. Så har skett i flera fall genom kompletterande förordningar. En myndighet som planerar att lämna ut uppgifter elektroniskt måste, när särskilda föreskrifter ges om sättet för utlämnande, bedöma om det informationsutbyte som planeras faller inom ramen för den särskilda regleringen i registerförfattning.

I flera registerförfattningar dras en skarp gräns mellan direktåtkomst respektive utlämnande på medium för automatiserad behandling. Högre krav brukar ställas vid direktåtkomst; jfr avsnitt 2.7. Dessa begrepp och när utlämnande på medium för a utomatiserad behandling kan anses föreligga i stället för direktåtkomst redovisas närmare i E-delegationens rapport Direktåtkomst och utlämnande på medium för automatiserad behandling.

Att särskilt observera: I en registerförfattning kan finnas särskilda regler som kan påverka en planerad it-baserad tjänst. Det kan t.ex. gälla:

- särskilda ändamålsbegränsningar, inklusive den s.k. finalitetsprincipen,
- särskilda begränsningar om utlämnande av uppgifter i elektronisk form,
- sökbegränsningar, och
- särskilda gallringsbestämmelser.

9.11 Vissa anknytande rättsfrågor

Sammanfattning: De juridiska förutsättningar som beskrivs i denna vägledning behöver beaktas tidigt i processen för att upphandla funktioner för en it-baserad tjänst. De juridiska kraven på den it-baserade tjänsten bör specificeras och tydligt framgå av upphandlingsunderlaget, så att leverantören måste uppfylla kraven. Vidare måste konkurrensrättsliga frågor övervägas om det finns risk för att myndighetens verksamhet kan snedvrida konkurrensen på marknaden.

9.11.1 Föreskrifter, avtal eller villkor i beslut för enskilda fall

Bakgrund

Frågan om viss myndighetsverksamhet ska anses vara av privat- eller offentligrättslig karaktär och om regler bör ges i författning eller genom avtal har varit föremål för utredning.[76] Där noterades att det förelåg osäkerhet om vissa dåvarande myndigheters (Postverkets och Televerkets) relationer till myndighetens kunder helt eller delvis var av offentligrättslig natur eller om de grundade sig på privaträttsligt avtal och att de val av juridisk lösning som dittills gjorts präglats av en slags vana. Utredningen fann att

- den bedrivna verksamheten liknade affärsverksamhet som privata företag driver,
- inget hindrade att kundvillkoren gavs formen av privaträttsliga avtalsvillkor och att förhållandet mellan myndighet och kund då skulle bedömas efter privaträttsliga regler
- det inte behövdes något bemyndigande för myndigheten att ställa upp villkoren eftersom avtalsvillkoren inte anses utgöra normer i regeringsformens mening, och

[76] Se Tele- och postkundsutredningen; se utredningens betänkande (SOU 1990:100) Avtalsvillkor eller föreskrifter – en rättslig översyn av postens och televerkets kundvillkor.

- även avgifterna inom området för dåvarande brevmonopol kunde bli att betrakta som privaträttsliga avtalsvillkor (SOU 1990:100; se bl.a. sammanfattningen s. 11 ff.).

Utredningen slutsats blev att privaträttsliga villkor borde användas så långt möjligt i en myndighets affärsverksamhet medan däremot föreskrifter måste användas när myndigheten utför uppgifter som innefattar myndighetsutövning. Utredningen konstaterade vidare att detta synsätt visserligen skilde sig från det som då varit det traditionella men att synsättet låg i linje med den utveckling som pågått (s. 192). Liknande bedömningar hade gjorts av regeringen i utredningens direktiv och i utskottsuttalanden till vilka det hänvisades i direktiven (dir. 1989:18, KU 1986/87:29 s. 39 och 73 och rskr. 226). Utvecklingen har fortsatt i samma riktning där it har införts.

Faktiskt handlande, ärendehandläggning och myndighetsutövning

Utöver en gräns mot vad som utgör privaträttslig verksamhet behöver en myndighets offentligrättsliga verksamhet delas in i handläggning av ärenden, utan eller med myndighetsutövning, och s.k. faktiskt handlande. När det rättsliga ramverket kring en myndighets it-baserade tjänster utformas behöver det övervägas om myndigheten genom en viss tjänst

1. tillhandahåller t.ex. en servicetjänst, en presentationstjänst, eller en bastjänst, och

2. utför faktiskt handlande eller ärendehandläggning, med eller utan myndighetsutövning.

Det bör samtidigt bedömas om flera av dessa tjänster och funktioner har integrerats.

Bemyndigande behövs för att bedriva verksamheten

En förvaltningsmyndighet under regeringen får agera endast inom ramen för sitt uppdrag från riksdag eller regering. Detta gäller oavsett om det är fråga om myndighetsutövning, ärendehandläggning eller faktiskt handlande.

Regeringen lämnar sina uppdrag till förvaltningen på olika sätt. I 5 § första stycket förvaltningslagen (2017:900) föreskrivs att en myndighet endast får vidta åtgärder som har stöd i rättsordningen. Bestämmelsen ger uttryck för legalitetsprincipen och tar sikte på de källor som tillsammans bildar rättsordningen i vidsträckt mening. Bestämmelsen innebär att det måste finnas någon form av normmässig förankring för all typ av verksamhet som en myndighet bedriver. Exempel på sådant författningsstöd kan vara allmänna bestämmelser i lag eller detaljerade regler i tillämplig speciallagstiftning. Det kan också vara fråga om allmänna eller särskilda bestämmelser i myndighetens instruktion eller myndighetsförordningen eller i någon annan förordning som regeringen har beslutat. Så kan t.ex. vara fallet i fråga om befogenheten för en myndighet att ingå civilrättsliga avtal eller annars uppträda som privaträttsligt subjekt. Legalitetskravet kan även vara uppfyllt genom ett förvaltningsbeslut, exempelvis om åtgärden har stöd i myndighetens regleringsbrev. Bestämmelsen innebär inte att varje enskild åtgärd som en myndighet vidtar måste ha uttryckligt stöd i en viss lagbestämmelse eller i andra föreskrifter som har meddelats i enlighet med 8 kap. RF (prop. 2016/17:180 s. 289).

Beträffande överlämnande av förvaltningsuppgift åt enskild krävs stöd i lag om uppgiften innefattar myndighetsutövning.[77]

Reglering på civilrättslig väg när så är möjligt

När en myndighet tillhandahåller en tjänst som lika gärna hade kunnat erbjudas av ett privaträttsligt subjekt bör regleringen ske genom civilrättsliga avtal, som myndigheten ingår med dem som vill använda tjänsten, inte genom författningsreglering. När myndigheter ingår sådana avtal måste regeringsformens krav på saklighet och opartiskhet iakttas.

Reglering genom föreskrifter eller beslut för enskilda fall

När en myndighet tillhandahåller en it-baserad tjänst i samband med myndighetsutövning eller annan förvaltningsverksamhet – som inte på samma sätt kan erbjudas av ett privaträttsligt subjekt – är verksamheten normalt redan reglerad i författning. Närmare regler kring en tjänst bör i ett sådant fall kunna ges genom villkor i förvaltningsbeslut för enskilda fall.

Samverkan mellan myndigheter under regeringen

Myndigheter under regeringen kan inte ingå civilrättsligt bindande avtal med varandra eftersom myndigheterna är en del av samma juridiska person. I praktiken formaliserar myndigheter dock sin samverkan genom överenskommelser även i sådana fall.

Till en myndighet kan också normgivningskompetens ha delegerats, så att mellanhavandet mellan myndigheter under regeringen kan regleras genom myndighetsföreskrifter. Uppdrag kan vidare ha lämnats i myndighetens instruktion, så att myndigheten kan fatta förvaltningsbeslut om mellanhavandet, där närmare regler ges genom villkor i beslut.

9.11.2 Immaterialrättsliga frågor

Innan en myndighet inför en it-baserad tjänst måste myndigheten säkerställa att de immaterialrättsliga frågorna har beaktats och att tillräckliga rättigheter finnas till själva e-tjänsten (källkod m.m.) och till e-tjänstens innehåll (text, bild m.m.).

Om den it-baserade tjänsten upphandlats bör därför i avtal föreskrivas antingen att rättigheterna till e-tjänsten överlåts till myndigheten eller att myndigheten ges en för ändamålet tillräcklig (i tid, användning m.m.) licens att nyttja tjänsten. Leverantören bör vidare ha en skyldighet att hålla myndigheten skadeslös för det fall tjänsten skulle visa sig göra intrång i tredje mans immaterialrätt.

I förhållande till it-baserade tjänster kräver immaterialrätten även att tillräckliga rättigheter måste finnas till innehållet i e-tjänsten. Om innehållet inte är skapat av myndigheten måste tillstånd från upphovsmännen finnas (med vissa undantag, t.ex. citat i enlighet med god sed).[78]

[77] Se 12 kap. 4 § RF och exempel tullens särreglering, se 2 kap. 4 § tullagen (2000:1281).

[78] Det har förekommit att offentlighetsprincipen använts för att mot upphovsmannens vilja framställa exemplar av och sprida upphovsrättsligt skyddade verk till allmänheten – se t.ex. om det s.k. scientologimaterialet. Visst skydd ges dock numera genom sekretessregleringen i 31 kap. 23 § OSL.

9.11.3 Upphandlings- och konkurrensrättsliga frågor

Upphandlingsrättsliga frågor

Avtal om varor eller tjänster som ingås av offentliga organ omfattas normalt av upphandlingslagstiftningen och ska föregås av en upphandling. Det finns olika upphandlingsförfaranden beroende på omfattning, typ av vara eller tjänst och belopp. Inom många områden finns också ramavtal som medför att myndigheten istället för att upphandla på egen hand kan avropa från befintliga avtal.

Det är av vikt att de juridiska förutsättningar som beskrivs i denna vägledning beaktas tidigt i processen för att upphandla funktioner för en e-tjänst. De juridiska kraven på den it-baserade tjänsten bör specificeras och tydligt framgå av upphandlingsunderlaget, så att leverantören måste uppfylla kraven.

Om flera myndigheter under regeringen samarbetar kring ett gemensamt allmännyttigt uppdrag, utan att blanda in något privat aktör, torde det dock ofta inte behöva genomföras någon upphandling.[79] Myndigheternas samarbete behöver emellertid formaliseras på lämpligt sätt.

Konkurrensrättsliga frågor

Konkurrenslagens (2008:579) bestämmelser kan bli tillämpliga även på offentliga organs agerande. Avtal, beslut eller samordnade förfaranden mellan företag som har till syfte eller resultat att hindra, begränsa eller snedvrida konkurrensen på marknaden är förbjudna.[80] Ett offentligt organ kan i en säljverksamhet förbjudas att tillämpa ett visst förfarande om detta snedvrider, eller är ägnat att snedvrida, förutsättningarna för en effektiv konkurrens på marknaden, eller hämmar, eller är ägnat att hämma, förekomsten eller utvecklingen av en sådan konkurrens.

Dessutom kan regler om statsstöd bli tillämpliga om ett offentligt organ utger stöd till ett företag. Ett stöd omfattas av statsstödsreglerna om detta gynnar ett visst företag, finansieras genom offentliga medel, snedvrider eller hotar att snedvrida konkurrensen samt påverkar handeln mellan EU:s medlemsstater.[81]

9.12 Rättsliga risker

I all verksamhet, såväl privaträttslig som offentligrättslig uppkommer risker till följd av att berörda författningar, avtal och överenskommelser inte är entydiga och klara. Reglerna måste därför tolkas. I traditionell miljö har de komplikationer som detta fört med sig kunnat hanteras efter hand eftersom manuell verksamhet smidigt kan anpassas till ny rättspraxis samt ändringar i lag, förordning, myndighetsföreskrifter och avtal. Författningsändringar har därför vanligtvis kunnat begränsas till att kodifiera redan utmejslade och vedertagna synsätt. Traditionellt utredningsarbete har vidare vilat på tydliga redovisningar av de praktiska förutsättningarna.

Vid verksamhetsutveckling inom e-förvaltningen är förutsättningarna vanligtvis helt andra. Informationssystem och ny infrastruktur behöver kravställas, byggas upp och i många fall upphandlas på förhand. I många fall har det varit svårt att kunna ge en tydlig beskrivning i alla delar. I fall där en juridisk tolkning därefter visat sig vara felaktig har i vissa fall synnerligen kostsamma nya utvecklingsinsatser visat sig nödvändiga. Det är av vikt att utredningar som

[79] Se prop. 2015/16:195 s. 402, jfr dock Kammarrätten i Stockholms dom (mål nr 7355-16) den 21 juni 2017 där en överenskommelse som Kungliga biblioteket ingått med Riksarkivet om digitalisering av pliktexemplar inte ansågs vara undantagen från upphandlingsplikt (ej prövningstillstånd i Högsta förvaltningsdomstolen).
[80] Överenskommelser om priser eller uppdelning av marknader utgör särskilt allvarliga konkurrensbegränsningar.
[81] Stöd av mindre betydelse anses inte påverka handeln inom EU och omfattas därför inte av statsstödsreglerna.

har i uppdrag att genomlysa centrala områden inom e-förvaltningen – så som handlingsoffentlighet, persondataskydd, myndighetssamverkan och upphandling – i tillräcklig omfattning beaktar den utveckling som i praktiken redan har ägt rum på it-området.

De rättsliga ställningstaganden som behöver göras för att nå regeringens förvaltningspolitiska mål har ofta fått göras inom varje projekt, utan det rättsliga stöd som brukar ges vid motsvarande anpassningar i traditionell miljö. De oklarheter som detta fört med sig vid tolkningen av bl.a. reglerna om personuppgiftsansvarets placering och möjligheterna att utkontraktera it-drift och andra tjänster behöver överbryggas. Denna vägledning är avsedd att utgöra en del i ett sådant arbete.

Att särskilt observera: Rättsliga risker kan aldrig helt undgås – inte ens om all verksamhetsutveckling med it-stöd får avvakta tillkomsten av en tydligare reglering. Myndigheterna behöver emellertid noggrant analysera och följa upp dessa risker, särskilt som utvecklingen är snabb inom området.

eSam 18-04

eSam är ett medlemsdrivet program för samverkan mellan myndigheter och Sveriges Kommuner och Landsting (SKL) för att underlätta och påskynda digitaliseringen inom det offentliga. Det bildades 2015 som en frivillig fortsättning på E-delegationen och bygger vidare på 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.

Vägledningarna finns tillgängliga på esamverka.se

I eSam ingår Arbetsförmedlingen, Bolagsverket, Boverket, Centrala Studiestödsnämnden, Domstolsverket, eHälsomyndigheten, Ekonomistyrningsverket, Försäkringskassan, Jordbruksverket, Kronofogdemyndigheten, Lantmäteriet, Migrationsverket, Naturvårdsverket, Pensionsmyndigheten, Polisen, Riksarkivet, Sida, Skatteverket, Skolverket, Sveriges Kommuner och Landsting, Statens servicecenter, Tillväxtverket, Trafikverket, Transportstyrelsen och Tullverket (mars 2018).

eSam