

Eget utrymme hos en myndighet

- En vidareutveckling





Innehåll

1.	Inledning	5
2.	Eget utrymme för individ och organisation	7
2.1	<i>Bakgrund</i>	7
2.2	<i>En vidareutvecklad användning</i>	8
2.3	<i>Krav på egna utrymmen</i>	9
2.4	<i>Utformningen av eget utrymme</i>	12
2.5	<i>Grundfunktioner i samspel</i>	13
	Åtgärd	13
	Funktion	13
2.6	<i>Olika typer av information</i>	14
2.7	<i>Anskaffning av flera tjänster samtidigt</i>	16
2.8	<i>Hos vem en tjänst finns</i>	17
2.9	<i>Gemensamma utrymmen</i>	18
3.	Juridisk bedömning	19
3.1	<i>Utrymmets och ytans juridiska status</i>	19
3.2	<i>Handlingsoffentlighet</i>	20
	3.2.1 En myndighet tillhandahåller utrymmet	20
	3.2.2 Driften av utrymmet utkontrakteras	23
	3.2.3 Invändningar som bedömts i lagmotiv och praxis	25
	3.2.3.1 <i>Tjänsteleverantören ska endast kunna ta del av den drifts- och säkerhetsrelaterade informationen</i>	25
	3.2.3.2 <i>Teknisk personal kan råka få se nyttoinformation</i>	26
	3.2.3.3 <i>Handlingar i olika utrymmen bedöms var för sig</i>	29
	3.2.3.4 <i>Gränserna måste upprätthållas även vid informationsutbyte</i>	30
	3.2.3.5 <i>Endast befordran av meddelanden för annan</i>	32
	3.2.3.6 <i>Hjälp-tjänster (support)</i>	32
	3.2.3.7 <i>Statistik och analysverktyg — flera tjänster anskaffas samtidigt</i>	34
	3.3 <i>Förvaltningslagen</i>	36
	3.3.1 Inkommande och service	36
	3.3.2 Service för att motverka fel och brister	38
	3.4 <i>Sekretess och tystnadsplikt</i>	40
	3.4.1 Utomstående ska inte ha insyn i eget utrymme	41
	3.4.2 Personalen ska ha tystnadsplikt	41
	3.4.3 En tystnadsplikt gäller normalt enligt lag	43
	3.4.4 Utlämnandefrågan — nationellt och internationellt	44
	3.4.4.1 <i>Myndigheten ska göra sekretessprövningen</i>	44
	3.4.5 Sekretessprövningen kan inte göras på förhand	45
	3.4.6 Röjande enligt OSL	45
	3.4.7 Legalitetsprincipen	47



3.4.8 Exit-frågan	48
3.5 <i>Bevarande och gallring</i>	49
3.6 <i>Skyddet för personuppgifter</i>	51
3.6.1 Vem är personuppgiftsansvarig?	52
3.6.2 Vad innebär myndighetens personuppgiftsansvar?	53
3.6.3 Vilket ansvar har innehavaren av utrymmet?	54
3.7 <i>Tillhandahållandet ska ingå i myndighets uppdrag</i>	54
3.8 <i>Reglering av egna utrymmen</i>	56
4. Praktisk utformning och användning	57
4.1 <i>Infrastruktur kring eget utrymme och programvaruföretag</i>	57
4.1.1 Digital årsredovisning — villkor godkänns i privat tjänst	58
4.1.2 Arbetsgivardeklaration – många roller, flera system kan ladda upp	59
4.1.3 Digital infrastruktur för återanvändning av uppgifter	61
4.1.4 Eget utrymme för företagsprofil — registrering för återanvändning	62
4.1.5 Sammansatta bastjänsten för grundläggande uppgifter (SSBTGU)	63



1. Inledning

Eget utrymme har utvecklats till en etablerad myndighetspraxis som fått allt större spridning. I anknytning till servicetjänster¹ och presentationstjänster² tillhandahålls eget utrymme och liknande funktioner för att innehavaren ska få automatiserad service och kunna hantera sina handlingar utan insyn av utomstående. Eget utrymme tillhandahålls numera dessutom åt andra myndigheter och åt företag som en vidareutveckling av eget utrymme för individ. I ett betänkande och flera vägledningar har E-delegationen och eSam redovisat sina juridiska bedömningar av denna hantering och en samsyn har efter hand vuxit fram kring dessa frågor.³

Utvecklingsarbetet har istället kommit att handla om de ytterligare funktioner som etableras kring eget utrymme och de möjligheter dessa funktioner ger att kommunicera och i övrigt underlätta enskildas kontakter med det allmänna. Denna vägledning tar därför sikte på denna utveckling och de möjligheter och risker som den kringliggande infrastrukturen för med sig.

Efter år 2016 då eSam publicerade ”[Eget utrymme hos myndighet — en vägledning](#)” har rättsläget vidare förtydligats genom rättspraxis⁴ och två lagstiftningsärenden där regeringen uttalat sig om hur eget utrymme förhåller sig till handlingsoffentlighet, offentlighets- och sekretesslagens regler om tystnadsplikt och förvaltningslagens regel om ankomstdag för handlingar.⁵ Dessutom har lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter trätt i kraft den 1 januari 2021. Visserligen ska den föreslagna lagen bara gälla när enskilda agerar som tjänsteleverantör, men uttalanden i lagmotiven ger ledning även vid leveranser från myndigheter.

Ref. 000001

¹ Med *servicetjänst* menas, enligt [Juridisk vägledning för verksamhetsutveckling](#) inom e-förvaltning 3.0, en e-tjänst där en innehavare av ett eget utrymme kan utforma utkast till handlingar i sitt utrymme, få uppgifter förfyllda eller annars utlämnade, antingen av den som tillhandahåller utrymmet eller annan med stöd av egen hämtning eller egen delning, sända handlingar till en mottagningsfunktion och vidta andra nödvändiga åtgärder, jfr avsnitt 4.2 i [prop. 2016/17:198](#).

² En *presentationstjänst* är, enligt nämnda vägledning, en e-tjänst där innehavaren av ett eget utrymme får handlingar visade utan att det som visas ska bli tillgängligt för andra, jfr avsnitt 4.5 i [prop. 2016/17:198](#).

³ Se SOU 2014:39, E-delegationens Juridiska vägledning för verksamhetsutveckling inom e-förvaltningen och eSams publikationer (se utöver den här uppdaterade vägledningen om eget utrymme hos myndighet), [Juridisk vägledning för verksamhetsutveckling](#) inom e-förvaltning 3.0, [Rättsligt uttalande](#) den 22 november 2017 Eget utrymme hos myndighet med tillhörande [Promemoria](#) den 10 november 2017 om eget utrymme, vägledningen Rättsliga förutsättningar för [digitalt i första hand](#), [Digitalisera rätt](#) — en praktisk juridisk vägledning (juni 2019) och en promemoria den 3 mars 2020 [Analysverktyg](#) och eget utrymme.

⁴ Se bl.a. [HFD 2018 ref. 48](#) och det s.k. VERA-målet, Kammarrätten i Jönköpings [mål nr 3610-19](#).

⁵ Se [prop. 2016/17:180](#) En modern och rättssäker förvaltning – ny förvaltningslag och [prop. 2016/17:198](#) Utökad sekretesskydd i verksamhet för teknisk bearbetning och lagring och den redovisning av dem som ges i [Promemorian](#) den 22 november 2017 om eget utrymme.



På uppdrag av regeringen tillhandahåller vissa myndigheter också tjänster åt andra myndigheter, ibland även åt företag, som delvis utgör en utkontraktering av it-drift. De grundläggande utgångspunkterna för denna hantering är visserligen desamma (se avsnitt 2.2), men de juridiska bedömningarna utfaller delvis på annat sätt för tjänster som innebär en utkontraktering. Sådana tjänster tillhandahålls dessutom i många fall som nationell digital infrastruktur vilken ska möjliggöra interoperabilitet och samverkan över myndighetsgränser. ”Utrymmen” som myndighet tillhandahåller åt (andra) myndigheter eller företag som en utkontraktering kallas i det följande ”lagringsytor” (jämför software as a service, SaaS, och liknande).

Medan de flesta myndigheterna behöver vägledning när det gäller eget utrymme (för individ och organisation) är kretsen av myndigheter som har att ta ställning till lagringsytor mera begränsad. De verksamhetsutvecklare, arkitekter och jurister med flera som har behov av vägledning är ofta inte heller desamma. Denna vägledning har därför begränsats till frågor om eget utrymme och tillhörande digital infrastruktur. Frågor om hur sådana funktioner etableras på ett rättsenligt sätt tas inte upp i denna vägledning utan i vägledningen Lagringsytor — infrastruktur för it-drift och samverkan.

I denna vägledning ges därmed en allmän beskrivning från en juridisk utgångspunkt av berörda funktioner (kap. 2). Den rättsliga genomgången begränsas däremot till en fördjupad analys av de tolknings- och tillämpningsfrågor som visat sig vara av särskild betydelse för den fortsatta utvecklingen av eget utrymme och den digitala infrastruktur som etableras kring dem (kap. 3). Vägledningen avslutas med exempel för att konkretisera de rättsfrågor som myndigheterna ställs inför när eget utrymme och tillhörande digital infrastruktur ska utvecklas och införas (kap. 4).

Arbetet med att ta fram vägledningen har genomförts av eSams rättsliga expertgrupp. Ledamöter i expertgruppen är Johan Bålman, Malgorzata Drewniak, Per Furberg, Erik Janzon, Gustaf Johnssén, Jan Sjösten, Gunnar Svensson och Christina Wikström. Adjungerade ledamöter i expertgruppen är Eva Maria Broberg Lennartsson, Veronica Eckerby, Linn Kempe och Maria Sertcanli.



2. Eget utrymme för individ och organisation

2.1 Bakgrund

Genom eget utrymme har en allmän tillit kunnat skapas till digitala tjänster. Tillsammans med funktioner för e-legitimering erbjuder dessa utrymmen en säker hantering och en förenklad vardag för enskilda. I den första versionen av denna vägledning begränsades de rättsfrågor som redovisades i huvudsak till funktioner som myndigheter tillhandahåller åt fysiska personer (*individer*) och till mera begränsade informationsutbyten än vad myndigheter numera inför via eget utrymme. Det har dessutom blivit vanligt att eget utrymme tillhandahålls åt myndigheter och företag⁶ (*organisationer*).

Eget utrymme och anknyttande funktioner har samtidigt blivit en central del i utvecklingsarbetet för att individer och organisationer ska kunna återanvända information och att myndigheter ska kunna samordna digitala tjänster, se bland annat verksamt.se och andra webbportaler där central tillgång ges till information och tjänster. För att samverkan ska fungera måste myndigheterna enas om hur informationsutbytet ska gå till och hur gemensamma säkerhetslösningar ska vara utformade. Detta inverkar på såväl informationshanteringen som arkitekturen och den juridiska lösningen, inte bara i egna utrymmen utan inom hela den digitala infrastruktur som berörs.

Denna vägledning ska ses som ett stöd vid vidareutveckling främst av den digitala infrastruktur som etablerats kring egna utrymmen för individ och för organisation. Det beskrivs hur eget utrymme och tillhörande digital infrastruktur kan användas på ett rättsenligt sätt över myndighetsgränser och hur funktionerna kan sättas in i sitt juridiska och tekniska sammanhang.

På uppdrag av regeringen tillhandahåller vissa myndigheter också tjänster åt andra myndigheter, ibland även åt företag, som delvis utgör en utkontraktering av it-drift (jfr software as a service, SaaS, och liknande) Som framgått tas emellertid frågor om hur sådana funktioner etableras rättsenligt inte upp i denna vägledning utan i vägledningen Lagringsytor — infrastruktur för it-drift och samverkan. Denna vägledning omfattar inte heller exempelvis funktioner för informationsförsörjning som myndigheter har i uppdrag att fullgöra inom särskilda områden och inte heller tillhandahållandet av öppna data.

⁶ Med företag menas här detsamma som i 1 kap. 2 § bokföringslagen (1999:1078).



2.2 En vidareutvecklad användning

Myndigheter har som framgått även börjat tillhandahålla eget utrymme åt (andra) myndigheter och företag. Mellan myndigheter och mellan myndigheter och företag sker informationsutbytet visserligen i många fall maskin till maskin via bastjänster, dvs. utan att tjänsten har ett användargränssnitt.⁷ Till eget utrymme hör normalt ett användargränssnitt.⁸ För ”utrymmen” som erbjuds till andra myndigheter eller till företag och som har användargränssnitt är likheten med eget utrymme *för individ* ofta så stor att de bör betecknas eget utrymme *för organisation*. Så är fallet när en myndighet som handlägger vissa ärenden tillhandahåller en digital tjänst åt myndigheter eller företag för att det ska bli enklare för dem att få information och att upprätta och ge in ansökningar, deklarerationer eller andra handlingar.

Skillnaden blir endast att det är *organisationen* (inte individen) som behöver *identifieras* på säkert sätt. Utrymmet har emellertid i båda fallen normalt ett användargränssnitt och är till för att ge service på motsvarande sätt som vid ett fysiskt besök hos berörd myndighet för att få enklare hjälp. En organisation kan dock vid besök i eget utrymme i många fall identifieras genom identifiering av servrar⁹, medan det i eget utrymme för individ normalt krävs att den fysiska person som innehar utrymmet identifieras, ofta med hjälp av en elektronisk identitet som innehåller personnummer. Eget utrymme brukar också förutsätta att individen loggar in med e-legitimation. En inloggning av en person till ett eget utrymme för organisation kräver även att det kontrolleras om den som legitimerat sig är behörig att företräda organisationen, se följande figur 10.¹⁰



Juridiska kontroller av behörighet att företräda berörd organisation och administration kring detta tillkommer alltså när det är en organisation som förfogar över ett eget utrymme. I övrigt kan de flesta rättsfrågorna lösas på samma sätt när utrymmet innehas av en individ respektive en organisation.

På uppdrag av regeringen tillhandahåller emellertid vissa myndigheter också tjänster åt andra myndigheter, i undantagsfall även åt företag, där utkontraktering av it-drift ingår (jfr software as a service, SaaS, och liknande). Tjänster av detta slag tillhandahålls

⁷ En bastjänst är en lagringsyta för uppgifter med ett eller flera applikationsprogrammeringsgränssnitt, API:er, som möjliggör åtkomst till uppgifter som finns på lagringsytan.

⁸ Viss integration med eget utrymme kan ske utan användargränssnitt, via API:er.

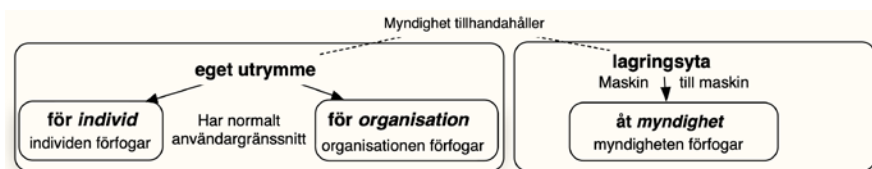
⁹ Så kan ske med hjälp av certifikat som identifierar respektive organisation som kommunicerar.

¹⁰ Behöriga företrädare loggar in via ett användargränssnitt, med stöd av uppgifter i publika register, fullmakter eller andra behörighetshandlingar.



dessutom i många fall som en nationell digital infrastruktur för att möjliggöra interoperabilitet och samverkan över myndighetsgränser.

För att inte blanda ihop eget utrymme (för individ eller organisation) med tjänster som myndigheter erbjuder åt andra myndigheter för it-drift, använder vi som framgått begreppet *lagringsyta* för de ”utrymmen” som en myndighet tillhandahåller åt andra myndigheter som en utkontraktering. De grundläggande utgångspunkterna beträffande handlingsoffentlighet och tystnadsplikt är visserligen desamma för denna hantering som beträffande eget utrymme, men de juridiska bedömningarna utfaller delvis på annat sätt för lagringsytorna. Informationsutbyte med stöd av lagringsytor sker dessutom maskin till maskin via bastjänster medan eget utrymme normalt har användargränssnitt. Detta hindrar dock inte att viss kommunikation med eget utrymme kan ske via API:er, se figuren.



Vi drar därmed en gräns i denna vägledning utifrån vem som har rätt att förfoga över ett eget utrymme respektive en lagringsyta och om det är en individ eller en organisation som förfogar över ett eget utrymme.¹¹ För att myndigheter som inför eget utrymme ska få en fullständig bild av den utveckling som skett kring eget utrymme ges även vissa beskrivningar av den digitala infrastruktur som krävs för att kommunicera rättsenligt med eget utrymme och hur gränser kan dras mellan de aktörer som brukar den.

Många frågor som rör lagringsytor kan visserligen lösas på samma sätt som för eget utrymme, men det finns skillnader som gör det ändamålsenligt att behandla eget utrymme och lagringsytor var för sig. Frågor som rör lagringsytor tas därför upp i en annan vägledning, *Lagringsytor — infrastruktur för samverkan*.¹²

2.3 Krav på egna utrymmen

I flera vägledningar har eSams redovisat de krav som ställs på ett eget utrymme, se exempelvis avsnitt 2.6 i [Digitalisera rätt](#) - en praktisk juridisk vägledning och de andra publikationer som nämns i fotnot 3 ovan. Vi upprepar inte alla dessa beskrivningar här. I [Juridisk vägledning för verksamhetsutveckling inom e-förvaltning 3.0](#) finns emellertid en uppräknning av de krav som bör ställas på eget utrymme för att

¹¹ Eftersom myndigheter vanligtvis inte tillhandahåller lagringsytor åt företag (jfr software as a service, SaaS, och liknande) berörs de särskilda frågor som detta aktualiserar endast marginellt.

¹² Lagg märke till att dessa indelningar tar sin utgångspunkt i vad som kan antas vara ändamålsenligt för att erbjuda vägledning till skilda kategorier av aktörer.



1. handlingar i ett utrymme inte ska bli allmänna,
2. ett tillräckligt sekretesskydd ska finnas,
3. hanteringen ska följa förvaltningsrättsliga, dataskyddsrättsliga och straffrättsliga regler, och
4. uppgifter i eget utrymme ska ges ett tillräckligt skydd från informationssäkerhetssynpunkt.

En bakgrund till denna uppräknig var regeringens uttalanden i lagmotiv om att det inte fanns vägledande avgöranden som ger tydligt besked beträffande vilka av de egna utrymmen som myndigheter tillhandahåller som uppfyller kraven i 2 kap. 13 § första stycket TF (prop. 2016/17:198 s. 10 f.). Följande krav redovisades av eSam ([Juridisk vägledning för verksamhetsutveckling inom e-förvaltning 3.0](#), s. 12 ff.):

Krav för att handlingar inte ska bli allmänna (2 kap. 13 § 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. Det behöver därför finnas återkommande åtkomskontroller.

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 skyddade mot insyn, jfr 40 kap. 5 § offentlighets- och sekretesslag (2009:400), i det följande OSL.¹³
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

¹³ I särskilda fall kan dock omedelbar gallring ge ett tillräckligt skydd, när det finns stöd för detta i beslut (för kommuner och regioner) eller i författning eller föreskrift om gallring från Riksarkivet (statliga myndigheter).



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.¹⁴
6. Tar användaren del av uppgifterna för en juridisk persons räkning bör användarens behörighet kontrolleras.

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.¹⁵
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.¹⁶
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.¹⁷
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.¹⁸
7. Identifiering och behörighetskontroll behöver utföras på ett säkert sätt.

¹⁴ Se beträffande denna hantering eSams publikation Juridisk vägledning för införande av [e-legitimering och e-underskrifter](#) 1.1.

¹⁵ 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](#) och en promemoria den 31 oktober 2017 [När har en handling kommit in till myndighet?](#)

¹⁶ I fotnoten hänvisades till denna vägledning i ursprungsversion.

¹⁷ Myndigheten har rätt att gallra nyttoinformation som oavsiktligt blivit allmän handling om det finns stöd för detta i beslut (för kommuner och regioner), författning eller föreskrift om gallring från Riksarkivet (statliga myndigheter). Utan sådant stöd får gallring inte ske (se avsnitt 3.5).

¹⁸ Se eSams rättsliga uttalande den 24 april 2017 [Missbruk av e-legitimation](#).



Informationssäkerhet och spårbarhet

Under denna rubrik hänvisade eSam

1. till kap. 5 i Juridisk vägledning för verksamhetsutveckling inom e-förvaltning 3.0, samt
2. anförde att behov av rensning och liknande åtgärder bör beaktas genom regler för eget utrymme så att eget utrymme inte kan missbrukas.

I det följande ska dessa krav genomlysas med utgångspunkt i rättspraxis, uttalanden i lagmotiv och utvecklingen av nya funktioner för egna utrymmen och lagringsytor. Dessa funktioner ska samtidigt sättas in i sitt sammanhang i syfte att utvecklingen av infrastruktur för offentlig verksamhet ska bygga på de krav som följer av Svenskt ramverk för digital samverkan.

2.4 Utformningen av eget utrymme

I anslutning till den i avsnitt 2.3 redovisade uppräknningen av krav på eget utrymme — hämtad från den [juridiska vägledningen för verksamhetsutveckling](#) — har eSam förklarat att rekvisiten för eget utrymme är utformade så att en myndighet kan tillhandahålla sådana även åt företag och andra myndigheter (vägledningen s. 13). Denna hantering har vuxit i en omfattning och med en variationsrikedom som vi inte kunnat förutse. Den inkluderar numera dessutom digital infrastruktur som gör det möjligt att kommunicera mera effektivt och att utbyta information via eget utrymme med stöd av en funktion för fråga- och svar så att individers och organisationers vardag kan förenklas ytterligare.

För att ge en fullständig bild av denna utveckling bör också det arbete nämnas som flera myndigheter bedriver för att tillhandahålla lagringsytor (jfr software as a service, SaaS, och liknande) åt andra myndigheter. Flera myndigheter har fått uppdrag av regeringen inom området. I förordning föreskrivs exempelvis att en myndighet ska eller får tillhandahålla tjänster som gäller administrativt stöd åt andra myndigheter,¹⁹ ge administrativt stöd och service åt domstolar,²⁰ utföra datorbearbetningar på uppdrag av myndigheter och enskilda samt tillhandahålla tjänster inom systemutveckling,²¹ lagra och tillgängliggöra information i enlighet med vad berörda parter kommer överens om och bedriva uppdragsverksamhet som omfattar tekniskt handläggningsstöd i förrättningsprocessen.²²

¹⁹ 1 § förordningen (2012:208) med instruktion för Statens servicecenter.

²⁰ 1 § förordningen (2007:1073) med instruktion för Domstolsverket.

²¹ 4 a § förordningen (2009:1174) med instruktion för Försäkringskassan.

²² 4 § andra stycket och 12 § 11 förordningen (2009:946) med instruktion för Lantmäteriet.



Ett vidgat stöd av detta slag innefattar vanligtvis utkontraktering av it-drift där en myndighet tillhandahåller lagringsytor och stödjande digital infrastruktur åt andra myndigheter. Funktioner av detta slag tillhandahålls inte som en del av tjänstelevererande myndighets allmänna serviceskyldighet enligt förvaltningslagen utan enligt särskilt uppdrag lämnat i förordning, regleringsbrev eller ett särskilt regeringsbeslut.

2.5 Grundfunktioner i samspel

Egna utrymmen och lagringsytor har tillsammans med tillhörande digital infrastruktur det gemensamt att de bygger på vissa (delar av) it-arkitekturer som används på ett likartat sätt. De används som grundfunktioner, som normalt inte är beroende av om det är ett eget utrymme eller en lagringsyta som erbjuds och inte heller av hur den tillhörande digitala infrastrukturen närmare utformas. Grundfunktionerna kan brukas generellt trots

Åtgärd	Funktion
En myndighet begär handlingar från en annan myndighet eller en enskild begär handlingar från annan, utan att detta sker genom direktåtkomst.	Fråga- och svarsfunktion jfr TF 2:6 & HFD 2015 ref. 61
Handling lämnas för befordran via infrastruktur som hör till utrymmen/lagringsytor utan att den som befordrar uppgifterna får ta del av eller annars bruka dem för egen räkning	Befordringsfunktion jfr TF 2:14 st 1 p 1 & prop. 2003/04:177 s. 17
Myndighet/individ/organisation hanterar information i en funktion hos annan myndighet där uppgifterna skyddas från utomstående	Eget utrymme eller lagringsyta jfr TF 2:13 och prop. 2016/17:198 s. 16
En enskild eller en myndighet tar emot handlingar digitalt som en enskild eller en myndighet har avsänt till annan.	Mottagningsfunktion jfr prop. 2016/17:180 s. 307, "på myndighetens server"
En myndighet sköter driften av nämnda funktioner åt en annan myndighet.	It-drift jfr TF 2:13
En myndighet hanterar information så att den blivit allmän handling och gallrar den genast för att skydda enskilda	Omedelbar gallring jfr TF 2:6
En innehavare av ett eget utrymme som från utrymmet begär uppgifter och får dem utlämnade direkt till sitt eget utrymme	Egen hämtning jfr TF 2:13 och TF 2:14 st 1 p 1
En innehavare av ett eget utrymme som genom en aktiv åtgärd eller automatiserat överför uppgifter från utrymmet till ett annat utrymme.	Egen delning jfr TF 2:13 och TF 2:14 st 1 p 1

Ref. 000001

den variationsrikedomen med vilket eget utrymme, lagringsytor och tillhörande digitala infrastruktur numera tillhandahålls av myndigheter.



I flera vägledningar har eSam närmare beskrivit dessa grundfunktioner, delvis med sikte på att de ska bli allmänt vedertagna rättsfigurer, se bland annat kap. 4 i [Juridisk vägledning för verksamhetsutveckling](#) inom e-förvaltning 3.0. Här finns inte utrymme att återge dessa beskrivningar. För att ge en grundläggande kännedom om de grundfunktioner som är av särskild betydelse för att upprätthålla de juridiska gränserna mellan olika myndigheter och andra organ redovisas emellertid följande sammanställning av dem.

En av dessa grundfunktioner innebär att handlingar begärs ut via en fråga- och svarsfunktion, en annan att en handling lämnas in till eller upprättas hos myndighet endast för befordran av meddelande. Ytterligare en grundfunktion innebär att handlingar förvaras hos myndighet endast som led i teknisk bearbetning och lagring för annans räkning. En annan grundfunktion används när en myndighet mottar handling.²³ Som grundfunktioner bör här även betraktas omedelbar gallring, ren it-drift, egen hämtning och egen delning, se följande sammanställning.

eSam har utvecklat dessa funktioner till ”byggklossar” som kan sättas samman på olika sätt utifrån de juridiska förutsättningarna i det enskilda fallet.

Ref. 000001

2.6 Olika typer av information

När ett eget utrymme och den tillhörande digitala infrastrukturen ska bedömas juridiskt behöver det också beaktas att det är *olika typer av information* som hanteras i eller i anknytning till dessa tjänster. I flera sammanhang — senast en promemoria från den 3 mars 2020, [Analysverktyg och eget utrymme](#) — har eSam utgått från en indelning i *nytt-, drifts- och säkerhetsrelaterad information*. Oberoende av om vi från juridiska utgångspunkter beskriver ett förvar av data som ett ”utrymme” eller en ”yta” går det inte att bortse från att informationshantering och kommunikation utförs genom it-system som har logiska gränser, inte fysiska, och att i vart fall en person på teknikavdelningen²⁴ måste kunna få åtkomst till ett system för att rätta fel i det och vidta nödvändiga åtgärder för informationssäkerheten.²⁵

I en proposition 2019/20:201 Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter, har regeringen uttalat bland annat att det under samtliga moment av teknisk bearbetning eller teknisk lagring kan förekomma att personal hos

²³ Att lämnas ut uppgifter genom direktåtkomst eller att lägga ut förvaltningsuppgifter som innefattar att en myndighet tar del av nyttoinformationen för en annan myndighets räkning är däremot sällan ändamålsenligt.

²⁴ Jfr hur detta uttryck används i prop. 2007/08:160 s. 71 och 164.

²⁵ Jfr SOU 2014:39 s. 25 där det anförts att nyttoinformation står för uppgifter som är till för enskilda eller befattningshavare till skillnad från drift- och säkerhetsrelaterad information som endast är till för tekniker.



tjänsteleverantören tar del av de uppgifter som hanteras för den uppdragsgivande myndighetens räkning. Detta kan enligt regeringen vara nödvändigt för att leverantören ska kunna utföra sina arbetsuppgifter som ett led i den tekniska bearbetningen eller tekniska lagringen samt att det normalt torde röra sig om *drifts- och säkerhetsrelaterad information*, t.ex. uppgifter om användarkonton, loggar, krypteringsnycklar, lösenord och säkerhetsinställningar (s. 23). Regeringen har emellertid tillagt att det också kan röra sig om *uppgifter i läsbar form* när hanteringen avser att endast tekniskt bearbeta eller tekniskt lagra uppgifter, jfr 4 § lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter.

E-offentlighetskommittén har på liknande sätt för sin juridiska bedömning identifierat tre skilda miljöer i en myndighets it-system (när behovet av undantag från handlingsoffentlighet för säkerhetskopior skulle övervägas). För det första *verksamhetsmiljön* där den vanlige datoranvändaren befinner sig och där *nyttoinformation* finns i form av ”originalhandlingar”, för det andra *driftmiljön* som innehåller information som har betydelse för driften av systemet, t.ex. olika slag av loggar, för det tredje *säkerhetskopiemiljön*, som endast har till syfte att garantera verksamhets- och driftmiljöns existens (SOU 2009:5 s. 106).

Dessa indelningar i miljöer och typer av uppgifter kan ytterligare behöva utvecklas när nya funktioner i eget utrymme eller inom den tillhörande digitala infrastrukturen ska sorteras in under gällande rätt. Enligt [Svenskt ramverk för digital samverkan](#) ska myndigheter bland annat (1) använda kontaktpunkter för organisationsövergripande processer,²⁶ (2) skapa e-tjänster i samverkan, (3) ge användare tillgång till personlig information om egna ärenden eller frågor, (4) efterfråga information bara en gång, (4) hämta information vid källan och (5) se till att informationen kan överföras.

Vid samverkan av detta slag uppkommer *it-miljöer där nya typer av information* hanteras för att egna utrymmen och tillhörande digital infrastruktur ska kunna utformas och användas på ett ändamålsenligt sätt. Generellt kan följande typer av uppgifter behöva hanteras.

- a) Uppgifter för *vägledning och guidning*, exempelvis metadata som gör det möjligt att hitta rätt bland olika tjänster²⁷ och guider och checklistor som sammanställer uppgifter åt den som använder en kontaktpunkt för organisationsövergripande processer så som [verksamt.se](#). Dessa metadata kan behöva hanteras på delvis annat sätt än själva nyttoinformationen. Exempelvis kan metadata som pekar ut

²⁶ En kontaktpunkt ger samlad information om processen, personlig vägledning, verktyg och tillgång till digitala tjänster. Offentliga organisationer ska bidra till att ge information om sin del i processen, bidra med underlag för guider och verktyg, samt tillgängliggöra sina tjänster för åtkomst via den gemensamma kontaktpunkten.

²⁷ Om användaren ska besöka ett flertal myndigheter tjänster och de har en viss komplexitet finns normalt behov av att lagra information om var användaren befinner sig i sin process i form av en individanpassad guide/checklista.



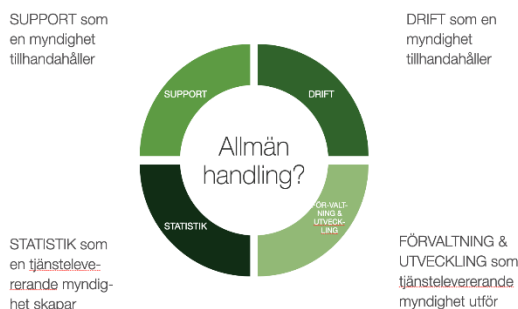
att uppgifter finns hos olika aktörer behöva samlas in på förhand så att nyttoinformationen vid behov kan sammanställas momentant i för användaren läsbar form.

- b) *Kontaktinformation*, exempelvis mobilnummer och e-postadress som behövs för att effektivt ge service åt enskilda och som idag inte har någon naturlig hemvist hos en myndighet. Uppgifter av detta slag behöver hanteras så att de inte blir föremål för missbruk, exempelvis genom att samlas in av aktörer som sänder eller möjliggör sändning av SPAM. Insamling och lagring av sådan information behöver ske skyddat samtidigt som sekretess normalt inte gäller om de ingår i en allmän handling.
- c) *Uppgifter i myndighetsregister*, dels s.k. grundläggande uppgifter som behövs i många sammanhang exempelvis om adress eller juridisk behörighet att företräda ett företag, dels djupare information exempelvis om fastigheter eller om ekonomiska förhållanden som kan behöva hämtas momentant från den bästa källan i stället för att lagras på flera ställen.

Vi återkommer till att olika slag av information och olika förvar för uppgifter behöver bedömas var för sig för att de i avsnitt 2.5 beskrivna grundfunktioner och den tillhörande digitala infrastrukturen ska kunna ges en rättsenlig utformning och regleras på ett ändamålsenligt sätt. Den närmare betydelsen från juridiska utgångspunkter av denna indelning redovisas genom de exempel som ges i kap. 4 på en rättsenlig användning av eget utrymme och tillhörande digital infrastruktur.

2.7 Anskaffning av flera tjänster samtidigt

När myndigheter anskaffar funktioner för eget utrymme och tillhörande digital infrastruktur påverkas de juridiska bedömningarna också av att en tjänst ofta anskaffas tillsammans med en eller flera andra tjänster från samma leverantör. Till egna utrymmen hör exempelvis ofta hjälptjänster (*support*), som kan kräva tillgång till viss information för att fungera effektivt. Det förekommer också att de anskaffas tillsammans med tjänster för *förvaltning och utveckling* eller att tjänstelevererande myndighet ska producera *statistik* för annans eller egen räkning, se figuren.



Risker har framträtt, vid anskaffningen av flera tjänster från samma leverantör, för att något led i hanteringen glömts bort vid den juridiska analysen. Hela verksamheten måste utformas så att gränserna mellan myndigheter eller andra organ inte bryts igenom eller suddas ut så att individers och organisationers arbetsmaterial blir allmänna handlingar.

2.8 Hos vem en tjänst finns

När egna utrymmen eller liknande funktioner införs behöver de utformas så att användare kan förstå var de befinner sig. Detta blir särskilt tydligt när flera myndigheter kan nås via samma ingångssida eller i anknytning till någon annan myndighetssamverkande kontaktpunkt som erbjuder egna utrymmen eller liknande funktioner via en tillhörande digital infrastruktur. Ställs från juridiska utgångspunkter frågan ”var” användaren befinner sig, avser den normalt vilken part som tillhandahåller eller annars ansvarar för den funktion som användaren för tillfället brukar. Eftersom det i digital miljö inte är fråga om några fysiska uppdelningar i fastigheter eller lokaler och användare inte heller kan kliva in i den digitala miljön för att orientera sig måste användaren utgå från vad som framgår av den texten, de ikonerna och de bilderna m.m. som presenteras i tjänstens användargränssnitt. Där tillhandahålls en slags ”karta” via vilken användare navigerar och ska kunna se vem som tillhandahåller vad.²⁸

Myndigheterna bör utgå från ett enhetligt synsätt och samordnade gränssnitt. Det blir annars svårt för användare att veta vilken aktör som tillhandahåller och ansvarar för en tjänst. Här bör traditionella fysiska gränser mellan de olika aktörernas verksamheter återskapas genom tydliga användargränssnitt där de *logiska* gränserna förenas med de *visuella* gränserna som på ett tydligt sätt visar vem som ansvarar för vad, jfr E-nämndens Vägledning (04:03) för användargränssnitt som uppfyller legala krav (dnr 2004/8-3).

²⁸ Är det en lagringsyta saknas användargränssnitt varför detta endast anges i lämnad information och de avtal som vanligtvis måste tecknas innan kommunikation kan ske maskin till maskin.



Med utgångspunkt härifrån bör en inloggning i en portaltjänst kunna visualiseras exempelvis som en dörr, knuten till en vaktkur där besökaren får legitimera sig, samt en trapp via vilken besökaren når olika lokaler och där viss ”gemensam” information presenteras. Användargränssnitten kan därmed utformas så att det tydligt framgår vilken aktör som användaren besöker och vem som ansvarar för tjänsten. En sådan utformning möjliggör rättsenliga myndighetsövergripande lösningar, se *bilaga*.

2.9 Gemensamma utrymmen

Utvecklingsarbetet inom EU och uppdrag i författning att utforma myndighetsamverkande kontaktpunkter och andra gemensamma funktioner för myndigheter och företag har fört med sig juridiska utmaningar. När olika myndigheter kan nås via samma ingångssida och eget utrymme kan erbjudas av flera myndigheter, så som exempelvis inom verksam.se, har diskussioner börjat föras kring något som ibland kallats gemensamt eget utrymme. Tanken verkar vara att innehavaren av utrymmet ska vara en och densamma medan flera myndigheter ska anses tillhandahålla utrymmet, jfr beskrivningen ovan av en portaltjänst visualiserad som en dörr knuten till en vaktkur där besökaren får legitimera sig. Väl inne i det gemensamma egna utrymmet ska användaren inte se olika lokaler utan bara ett enda myndighetsgemensamt utrymme. Att tekniskt utveckla funktioner för gemensamt eget utrymme är enkelt. Frågan är istället hur drift och förvaltning av gemensamma egna utrymmen ska kunna förenas med gällande rätt. Det juridiska ansvaret synes bli svårt att fördela mellan berörda organ eftersom rättsreglerna är utformade med utgångspunkt från att varje myndighet ska ansvara för sin förvaltningsverksamhet och sina tjänster — med undantag för information liknande en gemensam broschyr.

Mera konkret blir frågan vilken information i det gemensamma utrymmet som de olika myndigheterna ansvarar för att hålla uppdaterad med hänsyn tagen till exempelvis förändringar i myndigheters register. Vem ansvarar för förändringar av information och strukturer över tid när behov och krav ändras. Vem ansvarar juridiskt för att dessa förändringar görs i rätt tid och förhåller sig till eventuella författningsändringar? Vem svarar för att de harmonierar med den totala lösningen? Vilken part ska användaren vända sig till för att utkräva ansvar vid t.ex. en skada.

Till detta kommer frågor om vilken myndighet som ska pröva en begäran om en allmän handling eller sekretesspröva (olika delar av) den information som finns i utrymmet eller stå ansvarig enligt den författningsreglering som gäller för ärendehandläggning, dataskydd och informationssäkerhet. Gemensamma utrymmen kan skapa gränsdragningsfrågor och oklarheter i fråga om ansvaret mellan myndigheterna och ytterst i förhållande till den individ som använder utrymmet. Skulle myndigheter ändå



samverka så att de tillhandahåller gemensamma utrymmen måste det fastställas hur ansvaret fördelats och fördelningen måste kommuniceras med användarna så att ingen oklarhet kvarstår om vart användaren ska vända sig när denne vill utöva sina rättigheter enligt gällande rätt.

Dessa frågor behöver klargöras redan på designstadiet. Erfarenheten inom eSam har visat att det kan bli långsiktigt hållbart när varje myndighet själv har den juridiska rådgivningen över sina informationstillgångar och ”ensam” ska ansvara för funktioner som myndigheten tillhandahåller åt andra.

Samma funktionalitet kan dessutom normalt uppnås genom separata egna utrymmen för respektive myndighet, kombinerat med ett informationsutbyte som bygger på de grundfunktioner som har beskrivits i avsnitt 2.5, se även E-delegationens publikation [Fördjupning till Vägledning för digital samverkan](#) — Roller och överenskommelser (Version 4.1, 2015-05-28).

3. Juridisk bedömning

3.1 Utrymmets och ytans juridiska status

Ett eget utrymme ska anpassas till gällande rätt genom att konstrueras så att rekvisiten i vissa rättsregler uppfylls.

Ett eget utrymme ska utformas så att

- handlingar som hanteras där
 - behandlas endast som led i en teknisk bearbetning eller teknisk lagring för annans räkning (2 kap. 13 § första stycket TF),
 - inte anses ha kommit in till myndigheten eller nått en behörig befattningshavare (22 § FL),
- reglerna om dataskydd inte kräver att den myndighet som tillhandahåller utrymmet behöver ta del av de uppgifter som finns där,



- normalt ingen annan än den som innehar utrymmet får bereda sig tillgång till de uppgifter som finns där eller annars förfoga över informationen i utrymmet; se 4 kap. 9 a – 9 c §§, 10 kap. 5 § och 20 kap. 3 § brottsbalken,²⁹
- en handling som innehavaren har där omedelbart får gallras³⁰ om den råkat hanteras så att den blivit allmän (arkivförfattningar), och
- uppgifter som innehavaren har där eller som behandlas i anknytning till utrymmet endast för att upprätthålla en fungerande, effektiv och säker drift av eget utrymme är sekretessreglerade i den omfattning som behövs; jfr avsnitt 3.3.

I denna vägledning upprepar vi inte de allmänna genomgångar och checklistor som presenterats i äldre vägledningar. Framställningen begränsas till de juridiska frågor som har uppfattats som oklara och setts som hinder mot att använda eget utrymme, främst regler om offentlighet och sekretess, dataskydd, molntjänster och vissa förvaltningsrättsliga frågor. Inom dessa områden beskriver vi också

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

För den som vill få en allmän genomgång av egna utrymmen och hur de fungerar har eSam redan publicerat vägledningar och annat material.³¹

3.2 Handlingsoffentlighet

Ett eget utrymme ska utformas så att bara innehavaren får ta del av de uppgifter som finns där. Meningen är därför att uppgifter i egna utrymmen inte ska bli allmänna handlingar. Den juridiska bedömningen av om det finns risk för att allmänna handlingar uppkommer i eget utrymme blir styrande för utformningen av dem och ibland för hela den infrastruktur där sådana utrymmen ska ingå. I denna vägledning lägger vi därför särskild vikt vid dessa frågor.

3.2.1 En myndighet tillhandahåller utrymmet

Tillhandahåller en myndighet eget utrymme under sådana former att myndigheten får tillgång till innehavarens information *endast* som led i teknisk bearbetning eller teknisk

²⁹ Jfr dock vad som beskrivs om teknisk personals åtgärder för att exempelvis upprätthålla en tillräcklig säkerhetsnivå eller hantera en incident.

³⁰ Myndigheten har rätt att gallra nyttoinformation som oavsiktligt blivit allmän handling om det finns stöd för detta i beslut (för kommuner och regioner) eller i författning eller föreskrift om gallring från Riksarkivet (statliga myndigheter). Utan sådant stöd får gallring inte ske (se avsnitt 3.5).

³¹ Se [Juridisk vägledning för verksamhetsutveckling](#) inom e-förvaltning 3.0, [Rättsligt uttalande](#) den 22 november 2017 Eget utrymme hos myndighet med tillhörande [Promemoria](#) den 22 november 2017 om eget utrymme, vägledningen Rättsliga förutsättningar för [digitalt i första hand](#), [Digitalisera rätt](#) — en praktisk juridisk vägledning (juni 2019) och en promemoria den 3 mars 2020 [Analysverktyg](#) och eget utrymme. Det är också möjligt att orientera sig inom området genom att ta del av [en tidigare versionen av denna vägledning](#) (april 2016).



lagring för innehavarens räkning blir de handlingar som finns där inte allmänna. Skulle myndigheten för sin egen räkning använda information i eget utrymme blir den inte användarens ”egen”. Det behövs därför en tydlig gräns mellan handlingar som bara hanteras av utrymmesinnehavaren i utrymmet och handlingar som innehavarens har sänt från utrymmet till en myndighet.

Enligt 2 kap. 4 § TF är en *handling*³² allmän om den *förvaras* hos en myndighet och enligt 2 kap. 9 eller 10 § är att anse som *inkommen* till eller *upprättad* hos en myndighet. För digitala handlingar i ett eget utrymme gäller enligt 2 kap. 6 § TF att den anses *förvarad* hos en myndighet, om den är *tillgängliga* för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i uppfattbar form.³³

Information som innehavaren har i ett eget utrymme skulle alltså, om endast nämnda regler beaktas, bli allmän handling om utrymmet tillhandahålls av myndighet och innehållet inte krypteras eller på annat sätt görs tekniskt otillgängligt för myndigheten (se dock även avsnitt 3.2.2). Av 2 kap. 13 § första stycket TF följer emellertid att en handling som förvaras hos en myndighet *endast* som ett led i en teknisk bearbetning eller teknisk lagring för någon annans räkning inte anses som allmän handling hos den myndigheten.³⁴

Egna utrymmen ska vara utformade så att detta undantag blir tillämpligt på innehavarens information i utrymmet. Myndigheter som tillhandahåller eget utrymme måste därför se upp så att utrymmen inte får en felaktig utformning. Utför tillhandahållaren, eller driftsleverantören, andra åtgärder än teknisk bearbetning eller lagring är undantaget inte längre tillämpligt.³⁵ Innehavarens handlingar kan då bli allmänna och sakna skydd från insyn om de inte omfattas av sekretess.

Som exempel på teknisk *bearbetning* anges i de något ålderstigna förarbetena tryckning, kopiering, redigering av ljudupptagningar och överföring av sådana upptagningar till grammofonskiva (a. prop. s. 171 som hänvisar till s. 137). Som exempel på teknisk *lagring* anges sådana former av lagring som kräver tekniska anordningar, t.ex. lagring av information i skivminne eller på magnetband. Exakt vilka åtgärder som utgör enbart

³² Legaldefinitionen i 3 § av handling är utformad så att det knappast kan råda någon tvekan om att data i eget utrymme innefattas. ”Med handling avses en framställning i skrift eller bild samt en upptagning som endast med tekniska hjälpmedel kan läsas eller avlyssnas eller uppfattas på annat sätt.”

³³ Detta förvaringsrekvisit för elektronisk miljö har samordnats med en regel i 2 kap. 9 § första stycket TF om när en digital handling anses vara inkommen. Så anses vara fallet när någon *annan* har *gjort den tillgänglig* för myndigheten på det sätt som anges i 6 §; dvs. med *tekniskt hjälpmedel* som myndigheten *själv utnyttjar* för överföring i sådan form att den kan läsas, avlyssnas eller uppfattas på annat sätt. Cirkeln är därmed sluten. Är handlingen förvarad är den också inkommen, om ”någon annan har gjort den tillgänglig” på angivet sätt. Regeringen har förklarat att det räcker att en person hos myndigheten, t.ex. på teknikavdelningen, har tekniska möjligheter att överföra uppgifter i uppfattbar form för att sammanställningar av dessa uppgifter ska utgöra allmänna handlingar ([prop. 2007/08:160](#) s. 71).

³⁴ På motsvarande sätt följer det av 2 kap. 9 § tredje stycket TF att en handling som återkommer till en myndighet efter teknisk bearbetning eller teknisk lagring inte anses som en inkommen handling där. Detta undantag är av relevans om myndigheten anlitar en extern leverantör för drift av tjänsten. Rimligen bör den information som finns i eget utrymme, och som genom utkontrakteringen av it-driften görs tekniskt tillgänglig för denne, inte heller anses expedierad från, och därmed en upprättad allmän handling hos, den avsändande myndigheten. En annan tolkning skulle leda till att undantaget i 2 kap. 9 § tredje stycket TF skulle förlora sin funktion; jfr avsnitt 5.2 i [Outsourcing 2.0 En vägledning om sekretess och dataskydd](#).

³⁵ Detta gäller bara när hanteringen sker ”endast” som led i teknisk bearbetning eller teknisk lagring för annans räkning.



teknisk bearbetning eller teknisk lagring i dagens elektroniska verklighet är i någon mån osäkert. Regeringen har emellertid i prop. 2019/20:201 Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter (s. 22) förklarat att innebörden i lagförslaget av begreppen teknisk bearbetning eller teknisk lagring är densamma som i 2 kap. 9 § tredje stycket TF och 2 kap. 13 § första stycket TF. Beträffande vilka åtgärder som kan omfattas har regeringen anfört att tolkningen behöver göras i förhållande till dagens digitala informationshantering och den fortgående tekniska utvecklingen. En tjänsteleverantör kan exempelvis ha i uppdrag att införa, förvalta, utveckla och så småningom utveckla en tjänst åt en myndighet. Tjänsteleverantören kan under dessa olika faser behöva vidta en mängd olika åtgärder som innefattar teknisk bearbetning eller teknisk lagring av uppgifter för att upprätthålla den tillgänglighet, funktionalitet och prestanda i tjänsten som har avtalats mellan parterna. Det kan röra sig om förändring och tillägg i en befintlig tjänsts funktionalitet, etablering av en tilläggstjänst, integration mot andra tjänster, konfiguration, test och utveckling samt tillhandahållande av supporttjänster. Det kan också röra sig om säkerhetshöjande åtgärder som uppgradering, uppdatering, säkerhetskopiering, kryptering, anonymisering, pseudonymisering och incidenthantering. Vid utveckling av en tjänst kan myndighetens information behöva migreras eller exporteras tillbaka till myndigheten eller till en annan tjänsteleverantör.

Av praxis framgår att åtgärder som en myndighet till vilken utkontraktering skett utför *för egen räkning* och som innebär en *bearbetning av handlingarnas faktiska innehåll*, t.ex. genom att uppgifter används för framställning av statistik eller arbetsmiljörapporter, inte omfattas av undantaget ([HFD 2011 ref. 52](#)). Av praxis följer också att undantaget inte omfattar system där det saknas administrativa och tekniska begränsningar för den tjänstelevererande myndigheten att ta del av uppgifter i utrymmet/ytan i läsbart skick ([HFD 2018 ref. 48](#)).

Tjänster som en myndighet tillhandahåller elektroniskt och automatiserat för innehavararens räkning och som innefattar erforderliga tekniska begränsningar mot att en tjänstelevererande myndighet tar del av innehållet omfattas däremot av undantaget för endast teknisk bearbetning och lagring. Det innebär att ett exemplar av en handling som finns kvar i utrymmet kan ha mångfaldigats, så att ett annat exemplar med samma innehåll sänts till en myndighets elektroniska mottagningsställe och blivit allmän handling där.

I regeringens proposition 2019/20:201 Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter (s. 23) har regeringen uttalat att det under samtliga moment av teknisk bearbetning eller teknisk lagring kan förekomma att personal hos tjänsteleverantören tar del av de uppgifter som hanteras för den uppdragsgivande myndighetens räkning samt att detta kan vara nödvändigt för att de ska kunna utföra sina



arbetsuppgifter som ett led i den tekniska bearbetningen eller tekniska lagringen. Det torde enligt regeringen normalt röra sig om drifts- och säkerhetsrelaterad information t.ex. uppgifter om användarkonton, loggar, krypteringsnycklar, lösenord och säkerhetsinställningar, men det kan också röra sig om uppgifter i läsbar form. I den delen hänvisade regeringen till prop. 1975/76:160 s. 87 där det har uttalats att undantagen från offentlighet hos den myndighet som endast har en teknisk uppgift i sammanhanget ska gälla även för det fall att myndigheten såsom ett led i den tekniska bearbetningen för annans räkning har lov att överföra upptagningen i läsbar form.

Ett uppdrag som innehåller annat än enbart sådana tekniska moment faller dock utanför tillämpningsområdet för 2 kap. 13 § första stycket TF. I situationer där en myndighet rörande uppgifter utkontrakterar uppdrag av olika karaktär till samma tjänsteleverantör, t.ex. ett uppdrag som innebär att leverantören endast tekniskt bearbetar eller tekniskt lagrar uppgifter och ett annat uppdrag som omfattar åtgärder rörande uppgifterna som går utöver detta, är lagen om tystnadsplikt vid utkontraktering bara tillämplig i det förstnämnda fallet och bara på sådana uppgifter som inte dessutom hanteras inom ramen för det andra uppdraget (prop. 2019/20:201 s. 22).³⁶ Här blir det dock av betydelse att skilja mellan olika uppgiftssamlingar.³⁷

3.2.2 Driften av utrymmet utkontrakteras

Om en myndighet, som erbjuder egna utrymmen, utkontrakterar driften av dem har myndigheten normalt inte teknisk tillgång enligt 2 kap. 6 § TF till de handlingar som finns i dessa utrymmen. Är driftleverantören en myndighet kan det undantag från allmän handling som föreskrivs i 2 kap. 13 § första stycket TF tillämpas hos leverantören.

En myndighet kan i vissa fall låta en extern tjänsteleverantör sköta driften av egna utrymmen som myndigheten tillhandahåller åt andra. Sådan outsourcing eller utkontraktering är en del i myndigheternas strategier för att utveckla den digitala förvaltningen. När driften av eget utrymme har utkontrakterats finns de handlingar som innehavare hanterar i eget utrymme hos driftleverantören, inte hos den myndighet som i juridisk mening tillhandahåller utrymmet åt användaren. Av tekniska lösningar, outsourcingkontrakt och andra regler som rör ett utrymme kan följa att den myndighet som lagt ut driften inte har tillgång till information som förvaras i egna utrymmen.³⁸

³⁶ Regeringen har som framgått i prop. 2019/20:201 Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter (s. 22) förklarat att innebörden i lagförslaget av begreppen teknisk bearbetning eller teknisk lagring är densamma som i 2 kap. 9 § tredje stycket TF och 2 kap. 13 § första stycket TF.

³⁷ Se vidare vägledningen om Lagringsytor — infrastruktur som möjliggör interoperabilitet och samverkan, en promemoria den 3 mars 2020 Analysverktyg och eget utrymme, där eSam också konstaterar att den säkerhetsrelaterade och den driftrelaterade informationen ska bedömas för sig från offentlighets- och sekretessynpunkt och inte sammanblandas med användarens nyttoinformation i eget utrymme samt Kammarrätten i Jönköpings dom den 5 mars 2020 (mål nr 3610-19, det s.k. VERA-målet).

³⁸ Uppdraget till driftleverantören är alltså inte att upprätta eller annars hantera handlingar som tillhör myndigheten; jfr t.ex. RÅ84 2:49 och JO:s beslut den 23 januari 2014 (dnr. 3529-2012).



Under sådana förhållanden gäller istället huvudregeln i 2 kap. 6 § första stycket TF. Enligt den anses en upptagning bli allmän handling när den *är tillgänglig för myndigheten* med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att handlingen kan läsas, avlyssnas eller uppfattas på annat sätt.

En myndighet som erbjuder egna utrymmen bör alltså inte heller när driften av utrymmet är utkontrakterad ha tillgång till de handlingar som finns där. Detta bör återspeglas i de avtal och andra överenskommelser som träffas mellan den myndighet som tillhandahåller utrymmen och driftleverantören.³⁹ Att den myndighet som tillhandahåller eget utrymme elektroniskt, via t.ex. e-post, skulle kunna framställa en begäran om att vissa uppgifter ska lämnas ut ur ett utrymme innebär inte annat än att driftleverantören ska pröva frågan om och i så fall vilka uppgifter som ska lämnas ut – inte att begärande myndighet har teknisk tillgång till uppgifterna. Myndigheten får därmed, oberoende av om driften av utrymmet är utkontrakterad till en myndighet eller ett privaträttsligt organ, inte sådan tillgång till handlingar som avses i 2 kap. 6 § TF.⁴⁰

Det kan emellertid inte uteslutas att en *myndighet som tillhandahåller* egna utrymmen väljer en sådan utformning av it-driften att inte bara driftleverantören utan även myndigheten får anses förfoga enligt 2 kap. 6 § TF över frågan om och i så fall vilka uppgifter som ska lämnas ut. I så fall kan i stället 2 kap. 13 § första stycket TF bli tillämplig i enlighet med vad som har redovisats i avsnitt 3.2.1.

Är *driftleverantören* en myndighet eller ett annat organ hos vilket reglerna om handlingsoffentlighet gäller följer det av 2 kap. 13 § första stycket TF att handlingarna hos underleverantören inte blir att anse som allmänna där. Av outsourcingavtal och andra regler behöver följa att leverantören inte får använda uppgifterna för egen räkning och måste ha administrativa och tekniska begränsningar så att den tjänstelevererande myndigheten inte tar del av uppgifter i utrymmet i läsbart skick. – Aktörerna måste säkerställa att denna begränsning upprätthålls och att dessa krav blir tillgodosedda när berörda funktioner ska utformas, upphandlas, regleras och tas i drift, se vidare om upphandling avsnitt 2.9 i vägledningen Lagringsytor – infrastruktur för it-drift och samverkan.

³⁹ Användarvillkoren utgör en integrerad del av användaravtal som ingås av användaren av e-tjänsten. Att avtalsvillkoren utformas på ett korrekt och tydligt sätt är inte minst viktigt för att förhindra och beivra missbruk av e-tjänsten. Avtalet kan även tjäna som rättslig grund för personuppgiftsbehandling.

⁴⁰ Högsta förvaltningsdomstolen har i [HFD 2015 ref. 61](#) funnit att det inte finns sådan teknisk tillgång som avses i 2 kap. 6 § TF när en myndighet inte på egen hand kan söka i en annan myndighets uppgiftssamling, utan får framställa en begäran om att vissa uppgifter ska lämnas ut, och den myndighet som mottar begäran *förfogar över* frågan om och i så fall vilka uppgifter som ska lämnas ut.



3.2.3 Invändningar som bedömts i lagmotiv och praxis

Flera invändningar har gjorts över tid mot att eget utrymme skulle kunna införas med stöd av 2 kap. 13 § TF. Efter hand har det dock klarlagts att detta undantag från handlingsoffentlighet gäller när utrymmet och den kringliggande hanteringen utformats på ett ändamålsenligt sätt.

3.2.3.1 Tjänsteleverantören ska endast kunna ta del av den drifts- och säkerhetsrelaterade informationen

Tjänstelevererande myndighet måste såväl administrativt som tekniskt ha begränsat den egna personalens tillgång till uppgifterna. Personalen ska enbart kunna ta del av den drifts- och säkerhetsrelaterade informationen.

En myndighet som tillhandahåller eget utrymme får inte ta del av de handlingar som finns i utrymmet eftersom de finns där endast som ett led i teknisk bearbetning eller teknisk lagring för utrymmesinnehavarens räkning och därmed vara undantagna från handlingsoffentligheten, se HFD 2011 ref. 52. Där kunde dock den tjänstelevererande myndigheten enligt behörighetsvillkoren för den databas där uppgifterna förvarades ta del av uppgifterna i läsbart skick för att bl.a. framställa nationell statistik och rapportera till Arbetsmiljöverket. Eftersom uppgifterna var tillgängliga på detta sätt för den tjänstelevererande myndigheten ansågs de vara expedierade och därmed allmänna handlingar hos denne.

I [HFD 2018 ref. 48](#) klargjordes denna gränsdragning ytterligare. De aktuella handlingarna (avvikelse rapporter från privata utförare) fanns i den tjänstelevererande myndighetens verksamhetssystem. Dessutom hade personal hos tjänstelevererande myndighet tagit del av vissa handlingar och lagt uppgifter i dessa handlingar till grund för den statistik som den tjänstelevererande myndigheten tog fram. Högsta förvaltningsdomstolen fann att tjänstelevererande myndighet måste såväl administrativt som tekniskt ha begränsat den egna personalens tillgång till uppgifterna, så att dessa inte är tillgängliga i läsbart skick, för att rekvisitet ”endast” som led i teknisk bearbetning eller teknisk lagring för annans räkning ska vara uppfyllt: ”Myndighetens personal ska enbart kunna ta del av den drifts- och säkerhetsrelaterade informationen”, inte nyttoinformationen (se avsnitt 2.6). Tjänstelevererande myndighet måste alltså både administrativt och tekniskt begränsa den egna personalens tillgång till uppgifter som ska behandlas ”endast” tekniskt för annans räkning.

I [HFD 2018 ref. 48](#) var det emellertid fråga om information i myndighetens verksamhetssystem. För en uppgiftssamling som endast är avsedd för teknisk bearbetning och teknisk lagring för annan har i avsnitt 3.2.1 redovisats att det i lagmotiv



uttalats, dels att undantagen från offentlighet hos den myndighet som endast har en teknisk uppgift i sammanhanget ska gälla även för det fall att myndigheten såsom ett led i den tekniska bearbetningen för annans räkning har lov att överföra upptagningen i läsbar form (prop. 1975/76:160 s. 87), dels att det under samtliga moment av teknisk bearbetning eller teknisk lagring kan förekomma att personal hos tjänsteleverantören tar del av de uppgifter som hanteras för den uppdragsgivande myndighetens räkning och att detta kan vara nödvändigt för att de ska kunna utföra sina arbetsuppgifter som ett led i den tekniska bearbetningen eller tekniska lagringen (prop. 2019/20:201 s. 23). Regeringen förklarade samtidigt att det normalt torde röra sig om drifts- och säkerhetsrelaterad information, t.ex. uppgifter om användarkonton, loggar, krypteringsnycklar, lösenord och säkerhetsinställningar, men att det kan röra sig om uppgifter i läsbar form.

- Rättsliga risker — att hanteringen i någon del inte utförs ”endast” för annans räkning och att privat information därmed blir allmän.
- Vad som särskilt bör beaktas för att minimera risker — att uppgifterna inte får hamna i tjänstelevererande myndighets verksamhetssystem utan ska avskiljas fysiskt eller logiskt från tjänsteleverantörens egna informationstillgångar och att leverantörens egen personals tillgång till uppgifterna ska begränsas administrativt och tekniskt.
- Hur myndigheter kan förfara om en risk förverkligas — gallra omedelbart efter att kundens tillgång till dennes uppgifter säkrats (juridisk grund för detta behöver säkerställas på förhand).

3.2.3.2 Teknisk personal kan råka få se nyttoinformation

För att tjänstelevererande myndigheter ska kunna sköta it-system även när dessa system drabbas av tekniska fel eller angrepp måste några enstaka befattningshavare ha sådan åtkomst till eget utrymme att de kan råka få se nyttoinformation.

Så som informationstekniken är utformad måste några ha sådan övergripande teknisk behörighet att informationssystemen kan uppgraderas och i övrigt skötas exempelvis när de slutat att fungera eller har utsatts för attacker. I den första versionen av denna vägledning förklarades därför (avsnitt 5.3.2) att det inte kan uteslutas att personal som sköter driften av it-system där eget utrymme finns kan råka få se informationsinnehåll i ett eget utrymme, exempelvis när incidenthantering så kräver.

Har en teknisk befattningshavare råkat ta del av en uppgift, exempelvis i samband med att denne rättat ett fel i det tekniska systemet eller vidtagit en åtgärd som var nödvändig från informationssäkerhetssynpunkt, gäller ett förbud enligt 40 kap. 5 § OSL för denne



att röja uppgiften (tystnadsplikt). En förutsättning är dock att arbetet utförs i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning, dvs. inom samma tillämpningsområde som 2 kap. 13 § första stycket TF. Bestämmelsen i OSL gäller visserligen bara för uppgifter om enskildas personliga eller ekonomiska förhållanden. Om en uppgift istället är sekretessreglerad av hänsyn till ett allmänt intresse blir 11 kap. 4 a § OSL tillämplig, förutsatt att arbetet utförs i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning. En berättigad förväntan hos privatpersoner och företag, om att uppgifter som behandlas av en myndighet enbart som ett led i teknisk bearbetning för annan, ska vara skyddade från insyn eller utlämnande, kan därmed tillgodoses.

Frågan är dessutom om de tekniska och administrativa begränsningar som den tjänstelevererande myndigheten inför kan anses vara sådana som avses i [HFD 2018 ref. 48](#). Där framgår att tjänstelevererande myndighet ska, både administrativt och tekniskt, ha begränsat den egna personalens tillgång till de uppgifter som ska behandlas ”endast” tekniskt för annans räkning — den egna personalen ska enbart kunna ta del av den drifts- och säkerhetsrelaterade informationen. I det målet prövade Högsta förvaltningsdomstolen emellertid om handlingar i ett verksamhetssystem kan anses vara förvarade hos en myndighet endast som ett led i teknisk bearbetning eller teknisk lagring för annans räkning. Berörda handlingar hade således inte avskilts från myndighetens verksamhetssystem och de hade dessutom använts för den tjänstelevererande myndighetens egen räkning. Högsta förvaltningsdomstolen tog alltså ställning till om nyttoinformation i myndighetens verksamhetssystem, som vanliga handläggare hade tillgång till och delvis brukade för myndighetens egen räkning, var att anse som allmänna handlingar. Så är naturligtvis fallet.⁴¹

Beträffande uppgifter i eget utrymme som *avskilts* från myndighetens verksamhetssystem, har Kammarrätten i Stockholm i en dom den 26 oktober 2015 ([mål nr. 7369-15](#)) noterat att myndighetens handläggare *inte hade tillgång till eller använde sig av* berörda handlingar och inte heller använde dem för framställning av statistik eller liknande. Dessa handlingar var därmed inte allmänna enligt kammarrätten. Kammarrätten uttalade dessutom att det låg i sakens natur att vissa anställda hade åtkomst till den aktuella databasen för att administrera den.

En liknande bedömning har gjorts av kammarrätten i Jönköping i en dom den 5 mars 2020 ([mål nr 3610-19](#), ej prövningstillstånd, den s.k. VERA-domen). Där prövades

⁴¹ I [Juridisk vägledning för verksamhetsutveckling](#) inom e-förvaltning 3.0 har eSam, i den i avsnitt 2.3 återgivna uppräknigen av krav som bör ställas på eget utrymme, anfört att endast viss teknisk personal hos en myndighet som tillhandahåller eget utrymme får ha sådan behörighet att de kan bereda sig tillgång till uppgifter i eget utrymme och att sådan personal om de skulle råka läsa eller annars få del av information i eget utrymme, t.ex. när fel i system rättas eller åtgärder för informationssäkerheten vidtas, ska ha instruerats att sluta läsa innehållet och att inte lämna ut eller annars använda uppgifterna. När detta uttalades förelåg emellertid inte HFD 2018 ref. 48.



frågan om tekniska och administrativa begränsningar som införts var sådana som avses i [HFD 2018 ref. 48](#). Av redovisningen i kammarrättens dom framgick att informationen där var *logiskt* avgränsad och att det förelåg både tekniska och administrativa begränsningar. Dessutom tilldelades endast vissa medarbetare sådan särskild behörighet (central behörighet) att de kunde få *teknisk* åtkomst till berörda handlingar. Till detta kom den *administrativa* begränsningen att befattningshavaren måste få ett medgivande från den myndighet som nyttjade tjänsten och därefter genom en knapptryckning tilldela sig själv faktisk behörighet att komma åt den andra myndighetens handlingar i läsbar form. Kammarrättens fann att det inte var av avgörande betydelse vem som tar bort en teknisk begränsning när åtgärden förutsätter ett medgivande från den myndighet till vilken handlingen hör. Kammarrätten noterade vidare att medgivande kunde ges endast i syfte att ge teknisk support till den myndighet som anskaffat tjänsten.

Vem som anses ha förfoganderätten över handlingarna lyftes därefter fram av Kammarrätten som uttalade att det får förutsättas att en teknisk begränsning kan tas bort i de allra flesta fall och att det är av underordnad betydelse vem som gör det när det faktiskt är den myndighet som nyttjar tjänsten som beslutar om åtgärden genom att medge att den tjänstelevererande myndighetens personal får tillträde till systemet.

Kammarrätten fann därmed begränsningarna vara sådana som avses i 2 kap. 13 § första stycket TF och 40 kap. 5 § OSL. Denna bedömning vinner stöd av de ovan redovisade uttalandena regeringens proposition 2019/20:201 Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter (s. 22-23). eSam, som delar denna bedömning, vill betona vikten av att tekniska och administrativa begränsningar införts så att någon användning för myndighetens egen räkning inte kommer i fråga, jfr eSams publikation [Elektroniskt informationsutbyte](#) – en vägledning för utlämnande i elektronisk form, där funktioner förordats efter förebild av [HFD 2015 ref. 61](#).

- Rättsliga risker — att tekniska och administrativa begränsningar inte införts eller inte är sådana som beskrivs i [HFD 2018 ref. 48](#).
- Vad som särskilt bör beaktas för att minimera risker — att hanteringen utformas så att förfoganderätten över nyttoinformation alltjämt är kvar hos den som anlitat tjänstelevererande myndighet.
- Hur myndigheter kan förfara om en risk förverkligas — gallra omedelbart efter att kundens tillgång till dennes uppgifter säkrats (juridisk grund för detta behöver säkerställas på förhand).



3.2.3.3 Handlingar i olika utrymmen bedöms var för sig

Handlingar som finns i ett eget utrymme eller i myndighetens verksamhetssystem ska bedömas var för sig från offentlighets- och sekretessynpunkt.

Invändningar anfördes ursprungligen mot att tryckfrihetsförordningen skulle kunna tolkas på det sätt som E-delegationen och eSam hävdade. Det påstods bland annat att legalt utrymme inte skulle finnas för att ”isolera” ett tekniskt delmoment under den tid en handling förvaras hos en myndighet och betrakta detta separat. Undantaget i 2 kap. 13 § TF skulle ta sikte på hela den tid som myndigheten förvarar en handling. Det material som finns i *eget utrymme* och i myndighetens *verksamhetssystem* skulle ses som *en enhet*.⁴²

Regeringen använde sig emellertid av begreppet eget utrymme i det lagstiftningsärende genom vilket ett utökat sekretesskydd infördes och förklarade att *det finns stöd i rättspraxis* för att myndigheter tillhandahåller digitala tjänster som uppfyller kraven i 2 kap. 13 § första stycket TF.⁴³ Regeringen uttalade i detta sammanhang att det i stort helt saknas insynsintresse i sådan privat information som hanteras av myndigheten uteslutande för en enskilds räkning och som ofta sammanställs som ett led i framtagandet av handling som sedermera ska ges in till myndigheten. Denna bedömning stöds också av hur eget utrymme bedömts i rättspraxis (exempelvis i [HFD 2018 ref. 48](#)). På liknande sätt har i regeringens proposition 2019/20:201 Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter (s. 22-23) uttalats att, i situationer där en myndighet rörande uppgifter utkontrakterar uppdrag av olika karaktär till samma tjänsteleverantör, t.ex. ett uppdrag som innebär att leverantören endast tekniskt bearbetar eller tekniskt lagrar uppgifter och ett annat uppdrag som omfattar åtgärder rörande uppgifterna som går utöver detta, blir lagen (och därmed 2 kap. 13 § TF) bara tillämplig i det förstnämnda fallet och bara på sådana uppgifter som inte dessutom hanteras inom ramen för det andra uppdraget.

Ett och samma informationsinnehåll kan således finnas både i ett eget utrymme (utan att vara allmän handling där), och i en myndighets verksamhetssystem (som allmän handling), efter att den färdiga handlingen skickats till myndighetens funktion för att ta emot inkommande elektroniska handlingar. På samma sätt kan en handling som bevaras (i ett exemplar) i myndighetens verksamhetssystem lämnas ut till eget utrymme eller sändas via Min myndighetspost (i ett annat exemplar). Dessa olika exemplar av handlingar ska bedömas var för sig från offentlighets- och sekretessynpunkt. Detta gäller oberoende av om handlingar med samma innehåll finns i de olika utrymmen och

⁴² Se bland annat SOU 2013:80 s. 150 ff. och den närmare beskrivning av dessa invändningar som eSam redovisat på s. 17-18 i promemorian den 22 november 2017 Eget utrymme är numera accepterat i lagmotiv – men vilka juridiska krav ställs på eget utrymme? [fel version på nätet]

⁴³ Se prop. 2016/17:198 s. 7, s. 16, s. 19 och s. 20. Regeringen fann vidare E-delegationens förslag mera ändamålsenligt än de alternativ som framfördes i remissvar över berört utredningsförslag (a.prop. s 15 f. och s. 19).



verksamhetssystem etc. som ska bedömas var för sig. Detta har närmare beskrivits i en promemoria den 3 mars 2020 [Analysverktyg och eget utrymme](#), där eSam också konstaterat att den säkerhetsrelaterade och den driftrelaterade informationen ska bedömas för sig från offentlighets- och sekretessynpunkt och inte sammanblandas med användarens nyttoinformation i eget utrymme. Kammarrätten i Jönköping har på liknande sätt i en dom den 5 mars 2020 ([mål nr 3610-19](#), det s.k. VERA-målet) förklarat att varje del av det där berörda systemet och den information som en del innehåller måste prövas för sig (s. 10).

En myndighet som tillhandahåller egna utrymmen behöver alltså utforma uppgiftshandlingen så att det tydligt går att skilja mellan exemplar av en e-handling som finns i eget utrymme respektive i en mottagningsfunktion eller i ett verksamhetssystem hos myndigheten så att det tydligt går att skilja drift- och säkerhetsrelaterad information från nyttoinformation.⁴⁴ Detta blir av särskild betydelse när en myndighet, så som beskrivits i avsnitt 2.7, anskaffar flera tjänster samtidigt från en tjänsteleverantör.

- Rättsliga risker — att hantering och reglering utformas otydligt så att de olika kategorierna av information inte kan bedömas var för sig.
- Vad som särskilt bör beaktas för att minimera risker — att tydliggöra vilken hantering som förekommer och att reglera den så att det står klart vem som förfogar över olika kategorier av uppgifter.
- Hur myndigheter kan förfara om en risk förverkligas — gallra omedelbart efter att kundens tillgång till dennes uppgifter säkrats (juridisk grund för detta behöver säkerställas på förhand).

3.2.3.4 Gränserna måste upprätthållas även vid informationsutbyte

Myndigheterna bör införa funktioner för fråga och svar vid utbyte av uppgifter till och från egna utrymmen så att gränserna mellan olika aktörer och uppgiftssamlingar inte riskerar att brytas igenom.

Handlingar utbyts ofta till, från eller mellan egna utrymmen och myndigheters verksamhetssystem. I vissa fall utbyts information även med enskilda, företag och privatpersoner.

Av 2 kap. 6 § TF framgår att en handling (upptagning) anses vara förvarad hos en myndighet, om upptagningen är tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas eller avlyssnas eller uppfattas på annat sätt. Det finns därmed en risk för att

⁴⁴ Se eSams publikationer [Digitalisera rätt](#) — en praktisk juridisk vägledning, avsnitt 3.5.



informationsutbytet utformas så att uppgifter blir tillgängliga för ”fel” aktör och att gränserna mellan berörda aktörer därmed bryts igenom.⁴⁵ Vid exempelvis direktåtkomst uppkommer normalt omfattande överskottsinformation så att en digital tjänst inte kan genomföras på ett ändamålsenligt sätt (se SOU 2012:90).

Utformas funktionerna istället för utlämnande på medium för automatiserad behandling uppkommer inte dessa komplikationer. Frågan om när direktåtkomst ska anses föreligga klargjordes genom [HFD 2015 ref. 61](#). Där fann Högsta förvaltningsdomstolen att det inte finns sådan teknisk tillgång som avses i 2 kap. 6 § TF när en myndighet inte på egen hand kan söka i en annan myndighets uppgiftssamling, utan får framställa en begäran om att vissa uppgifter ska lämnas ut, och den myndighet som mottar begäran *förfogar över* frågan om och i så fall vilka uppgifter som ska lämnas ut. Att denna bedömning inte bara omfattar socialförsäkringsdatabasen utan gäller generellt framgår av Högsta förvaltningsdomstolens domskäl i HFD 2020 not 16.

Hur funktioner för informationsutbyte på medium för automatiserad behandling kan utformas för att bli rättsenliga har närmare beskrivits i eSams publikation [Elektroniskt informationsutbyte](#) – en vägledning för utlämnande i elektronisk form. Resultatet har blivit en grundfunktion eller ”byggkloss” i form av en fråga- och svarsfunktion som införts av flera myndigheter. Ett informationsutbyte kan på detta sätt inordnas under gällande rätt utan att gränserna mellan olika myndigheter och uppgiftssamlingar bryts igenom. Myndigheterna bör bruka dessa juridiska lösningar och (delar av) it-arkitekturer för kommunikation med egna utrymmen.

- Rättsliga risker — att hantering utformas så att direktåtkomst uppkommer och att de uppgifter som hanteras för annan myndighet anses expedierade av denna myndighet och inkomna hos tjänsteleverantören utan att något undantag från handlingsoffentlighet gäller.
- Vad som särskilt bör beaktas för att minimera risker — att säkerställa att en sådan fråga- och svarsfunktion föreligger som HFD avsett.
- Hur myndigheter kan förfara om en risk förverkligas — gallra omedelbart efter att kundens tillgång till dennes uppgifter säkrats (juridisk grund för detta behöver säkerställas på förhand).

⁴⁵ Av prop. 2007/08:160 s. 71 och s. 164 framgår att det räcker att det finns en person hos den mottagande myndigheten, t.ex. på teknikavdelningen, som har tekniska möjligheter att överföra en upptagning till sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas för att den ska utgöra allmänna handlingar hos den mottagande myndigheten.



3.2.3.5 Endast befordran av meddelanden för annan

Handlingar som lämnats in till eller upprättats hos en myndighet endast för befordran av meddelande är enligt 2 kap. 14 § första stycket 1 TF inte allmänna hos den förmedlande myndigheten.

Ett brev, ett telegram eller någon annan sådan handling som har lämnats in till eller upprättats hos en myndighet endast för befordran av ett meddelande anses enligt 2 kap. 14 § första stycket 1 TF inte vara allmän handling. Lagtextens ordalydelse talar för att bestämmelsen bara är tillämplig när myndighetens befattning med ett brev är begränsad till att vidarebefordra detta till någon (prop. 1975/76:160 s. 171 ff.). I [HFD 2019 ref. 29](#) fann HFD att detta undantag från allmän handling inte var tillämpligt på en av Kriminalvården granskad och kvarhållen försändelse till en intagen eftersom den befordran som ägde rum var förenad med myndighetsutövning.

Vid ren förmedling är situationen en annan. En myndighet som bara tillhandahåller vidareförmedling av meddelanden — exempelvis så att information kan begäras från den ursprungliga källan — får inte ta del av försändelserna utan bara vidarebefordra dem. Här motsvarar förutsättningarna dem som regeringen tog ställning till i propositionen 2003/04:177 Ändringar i mönsterskyddslagen på grund av EG-förordningen om gemenskapsformgivning. Där uttalade regeringen att handlingar som kommer till Patent- och registreringsverket för att vidarebefordras av verket till en Byrå för harmonisering inom den inre marknaden inte är att anse som allmänna handlingar hos Patent- och registreringsverket. I korthet var skälen att Patent- och registreringsverket endast skulle motta ansökningshandlingarna för vidarebefordran och varken skulle eller fick göra någon materiell eller formell prövning; verket skulle endast märka och vidarebefordra försändelserna. Dessa handlingar bedömdes inte vara allmänna hos vidarebefordrande myndighet trots att de öppnas och stämplas av handläggare som vidarebefordrar dem.⁴⁶

De handlingar som är under befordran inom en sådan infrastruktur ska alltså bedömas för sig från offentlighets- och sekretessynpunkt. De rättsliga risker och behov av åtgärder som uppkommer är desamma som i avsnittet ovan.

3.2.3.6 Hjälpjänster (support)

Sätts de grundfunktioner som beskrivits i avsnitt 2.5 samman på ett ändamålsenligt sätt kan information i ett eget utrymme lämnas ut till en hjälpjänst genom en fråga- och

⁴⁶ Regeringen anförde vidare följande: Patent- och registreringsverkets befattning med de handlingar som skall vidarebefordras till byrån i Alicante kan inte jämföras med vårdmyndigheters hantering av post till intagna och kan inte anses utgöra någon form av myndighetsutövning från Patent- och registreringsverkets sida med avseende på innehållet i handlingarna. Av motiven till bestämmelsen i 2 kap. 11 § (numera 13 §) 1 tryckfrihetsförordningen framgår vidare att bestämmelsen motiverades av att det vid post- och telegrambefordran inte fanns något insynsintresse (a. prop. s. 172). Motsvarande gäller beträffande innehållet i de ansökningshandlingar som skall vidarebefordras till byrån i Alicante. Innehållet i handlingarna är avsett för byrån och skall och får endast behandlas av byrån (a.prop. s. 17).



svarstjänst. De exemplar av handlingar som finns kvar i utrymmet omfattas därmed alltjämt av undantaget i 2 kap. 13 § första stycket TF från offentlighetsinsyn.

Myndigheter som tillhandahåller egna utrymmen får som framgått inte ta del av eller annars använda eller förfoga över de uppgifter som finns där för egen räkning ([HFD 2011 ref. 52](#) och [HFD 2018 ref. 48](#)). Frågan uppkommer därmed hur de ska kunna ge hjälp i de fall där detta kräver tillgång till information som finns i ett utrymme.

Regeringen har uttalat att 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.⁴⁷

I [Juridisk vägledning för verksamhetsutveckling](#) inom e-förvaltning 3.0 (avsnitt 8.1) har eSam beskrivit de olika typer av hjälptjänster som brukar förekomma. Här berörs inte de tjänster där hjälpsökande myndighet och den myndighet som ger hjälp kommunicerar endast muntligt. Inte heller de där hjälpsökande myndighet lämnar ut en skärmdump från sitt eget utrymme till hjälpfunktionen som skyddas genom att gallras (enligt gallringsbeslut) när hjälpen getts så att informationen förblir skyddad.

I samma vägledning har emellertid också beskrivits hur utrymmesinnehavare lämnar vissa uppgifter eller all nyttoinformation i eget utrymme till en myndighets hjälpfunktion så att supportärendet kan genomföras digitalt – i samverkan mellan innehavaren och befattningshavaren i hjälptjänsten. Enligt vägledningen skulle utrymmet därefter avslutas på grund av att materialet i utrymmet sades bli allmän handling. Ett nytt (skyddat) eget utrymme skulle därefter kunna skapas för innehavaren.

Frågan är emellertid om denna försiktiga bedömning är korrekt. Sätts de grundfunktioner (pusselbitar) som beskrivits i avsnitt 2.5 samman på ett ändamålsenligt sätt kan information i ett eget utrymme eller en lagringsyta lämnas ut endast genom en fråga- och svarstjänst. Den som ger hjälp får inte direktåtkomst till utrymmet utan nya exemplar av de utlämnande handlingarna förvaras i den hjälpgivande myndighetens verksamhetssystem för hjälptjänsten. Innehavaren av utrymmet förfogar alltså alltjämt ensam över den information som finns i utrymmet och bestämmer ensam över vad som ska lämnas ut eller annars göras tillgängligt därifrån via fråga- och svarstjänsten. De exemplar av handlingar som finns kvar i utrymmet och de som överförs från utrymmet

⁴⁷ Prop. 2016/17:198 s. 24. Regeringen har samtidigt 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 (a.prop. s. 8).



via en befordringsfunktion och nått verksamhetssystemet hos den myndighet som ger hjälp ska som framgått bedömas var för sig från offentlighets- och sekretessynpunkt.

Det egna utrymmet förblir därmed intakt från offentlighets- och sekretessynpunkt genom att undantaget i 2 kap. 13 § första stycket TF alltjämt är tillämpligt på handlingarna i utrymmet. Bara de exemplar som lämnas ut till hjälptjänsten blir allmän handling.

Kammarrätten i Jönköping synes visserligen ha gått ett steg längre i det s.k. VERA-målet ([mål nr 3610-19](#)) genom att anse att tjänstelevererande myndighets personal kan bistå en myndighet, till vilken den tillhandahåller *it-drift, även med supporttjänster* som innefattar korrigeringar och felavhjälpning så att tillgång ges för detta även till nyttoinformation i lagringsytor. Felskickade handlingar kunde därmed tas bort från lagringsytan av tjänstelevererande myndighets personal. Enligt eSams bedömning är det dock lämpligt att överväga en mera försiktig hållning i avvaktan på att frågan blir ytterligare prövad, när det är möjligt att ge den efterfrågade hjälpen utan att tjänsten leverantörens befattningshavare får tillgång till utrymmet.⁴⁸

Genom att sätta samman de grundfunktioner som beskrivits i avsnitt 2.5 på ett ändamålsenligt sätt kan alltså information i ett eget utrymme lämnas ut till en hjälptjänst genom en fråga- och svarstjänst, så att de exemplar av handlingar som finns kvar i utrymmet alltjämt omfattas av undantaget i 2 kap. 13 § första stycket TF från offentlighetsinsyn.

- Rättsliga risker — att hantering utformas så att direktåtkomst uppkommer och att uppgifter i egna utrymmen blir allmänna handlingar hos tjänstelevererande myndighet.
- Vad som särskilt bör beaktas för att minimera risker — att säkerställa att en sådan fråga- och svarsfunktion föreligger som HFD avsett och att annan åtkomst inte ges.
- Hur myndigheter kan förfara om en risk förverkligas — gallra omedelbart uppgifter i utrymmet efter att kundens tillgång till uppgifterna har säkrats (juridisk grund för detta behöver säkerställas på förhand).

3.2.3.7 Statistik och analysverktyg — flera tjänster anskaffas samtidigt

För att myndigheter ska kunna införa enklare, tydligare och mera ändamålsenliga digitala tjänster behövs teknisk och administrativ information om hur tjänsterna fungerar och

⁴⁸ Se även Kammarrätten i Stockholms [mål nr. 7369-15](#) där kammarrätten uttalade att det låg i sakens natur att vissa anställda hade åtkomst till den aktuella databasen för att administrera den.



används. Sådan information behövs ofta även för statistiska ändamål eller för att fördela kostnader mellan aktörerna som brukar en digital tjänst.

De frågor detta för med sig från offentlighetssynpunkt har nyligen genomlysts i en promemoria av eSam den 3 mars 2020 [Analysverktyg och eget utrymme](#). eSams rättsliga expertgrupp har där förklarat att uppgifter som uppstår i anknytning till e-tjänster kan brukas av myndigheten för egen räkning utan att uppgifter i användares eget utrymme hamnar utanför tillämpningsområdet för 2 kap. 13 § första stycket TF, förutsatt att uppgifterna inte hämtas från nyttoinformation i eget utrymme och att myndigheten har begränsat den egna personalens tillgång till nyttoinformationen i eget utrymme (jfr HFD 2018 ref. 48). I promemorian finns dessutom fem praktiska exempel på vad som är tillåtet och vad som inte är det.

Vad som sagts ovan om att en fråga och svarstjänst kan användas, utan att andra uppgifter än dem som lämnats ut blir allmänna hos avsändare eller mottagare, gäller alltså även om ändamålet är att ta fram statistik eller att använda ett analysverktyg. En likartad bedömning har dessutom gjorts av Kammarrätten i Jönköping som, beträffande domstolars data hos Domstolsverket, uttalat att varje del av systemet och den information den delen innehåller prövas för sig. Det förhållandet att vissa av Domstolsverkets anställda hade en mer fri tillgång till den del av systemet som genererade uppgifter som används för att ta fram statistik innebar inte att de handlingar som fanns i systemet i läsbart skick blev allmänna handlingar hos Domstolsverket ([mål nr 3610-19](#), ej prövningstillstånd, den s.k. VERA-domen).

Vi förordar att denna gräns mellan uppgiftssamlingar säkerställs genom att utlämnandet av uppgifter till en uppgiftssamling för statistik, när så är möjligt, äger rum via en tjänst för fråga och svar (jfr ovan vid fotnot 36). Detta behov blir särskilt tydligt när en myndighet, så som beskrivits i avsnitt 2.7, anskaffar flera funktioner från en och samma leverantör. De rättsliga risker och behov av åtgärder som uppkommer är desamma som i avsnittet ovan.

Checklista för handlingsoffentlighet:

- Kan myndigheten genom kryptering eller annan teknisk lösning utforma eget utrymme så att informationen i utrymmet inte blir tekniskt tillgänglig enligt 2 kap. 6 § TF för någon inom myndigheten, inte ens för tekniker med högsta behörighet i myndighetens it-miljö?
- Kan myndigheten – om ett heltäckande hinder mot teknisk åtkomst för myndighetens personal inte går att införa – begränsa åtkomsten så att

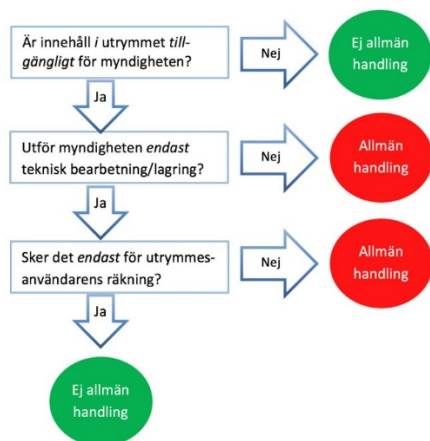


informationen bara används för teknisk lagring och teknisk bearbetning för annans, inte för egen, räkning?

- Är personalens hantering av uppgifter i eget utrymme tydligt reglerad och finns tillräckliga tekniska hinder mot åtkomst för personalen?
- Utkontrakteras driften av eget utrymme? Har den tekniska hanteringen och avtalen i så fall utformats så att handlingar i eget utrymme, som finns hos driftleverantören, inte är tillgängliga för den myndighet som erbjuder eget utrymme åt användare?
- Finns det någon plan för hur myndigheten ska agera för att skydda enskilda om hanteringen av eget utrymme skulle falla så att handlingar oavsiktligt blir allmänna?
- Finns det en tydlig punkt för att sända iväg handling från eget utrymme och tydliga avgränsningar i övrigt så att det inte kan finnas någon tvekan om vad som är användarens material respektive myndighetens material?

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

Ref. 000001



Figur över frågor rörande handlingsoffentlighet

3.3 Förvaltningslagen

3.3.1 Inkommande och service

Enligt förvaltningslagen (2017:900) har en handling kommit in till en myndighet den dag som handlingen når myndigheten eller en behörig befattningshavare. I it-miljö betyder detta att en handling kommer in när den blir tillgänglig på myndighetens server. Denna



nya reglering innebär, på samma sätt som enligt äldre rätt, att en elektronisk handling kommer in till myndighet den dag som handlingen når den funktion där myndigheten tar emot sådana försändelser. Myndigheten bör anvisa en mottagningsfunktion dit meddelanden kan sändas, skicka kvittens när ett meddelande nått dit och underrätta avsändaren om mottaget meddelande inte har kunnat uppfattas.

Enligt 6 § förvaltningslagen (2017:900; FL) ska en myndighet ska se till att kontakterna med enskilda blir smidiga och enkla. Myndigheten ska vidare lämna den enskilde sådan hjälp att han eller hon kan ta till vara sina intressen. Bestämmelsen är tydligare formulerad än i äldre förvaltningslag för att rätten att få hjälp är inte ska vara begränsad till en viss form. För faktiskt handlande av detta slag, t.ex. att tillhandahålla tekniskt och administrativt stöd för att enskilda ska kunna ge in handlingar digitalt, gäller FL:s regler om service. Hjälpen ska enligt 6 § FL ges i den utsträckning som är lämplig med hänsyn till frågans art, den enskildes behov av hjälp och myndighetens verksamhet.

I [Juridisk vägledning för verksamhetsutveckling](#) inom e-förvaltning 3.0 (avsnitt 4.1.4) har eSam beskrivit detta så att en handling i ett eget utrymme hanteras i ett *serviceskede*, dvs. ett skyddat förlopp där en användare hanterar uppgifter så att service ges enligt FL och ingen utomstående avses ha insyn i de uppgifter som behandlas där. Av vägledningen framgår också att (ett exemplar av) en handling som finns i en användares eget utrymme inte är föremål för en myndighets handläggning av ett förvaltningsärende. Handlingen är inte att anse som inkommen till myndighet.⁴⁹ Denna bedömning har gjorts enligt en sedan länge etablerad myndighetspraxis.

Enligt 22 § FL har en handling kommit in till en myndighet den dag som handlingen når myndigheten eller en behörig befattningshavare. För ingivning i anknytning till digitala 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 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. När innehavaren av ett eget utrymme eller en lagringsyta bestämmer sig för att lämna in en handling genom att på ett aktivt och medvetet sätt avsända den till en myndighets mottagningsställe blir en handling som nått dit inkommen i förvaltningslagens mening.

⁴⁹ Se även [Juridisk vägledning för verksamhetsutveckling](#) inom e-förvaltning 3.0 (avsnitt 9.9).



Myndigheternas mottagningsfunktioner bör utformas så att kvittens sänds när en försändelse 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.

3.3.2 Service för att motverka fel och brister

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

Service kan erbjudas helt automatiserat i användares eget utrymme, utan att handlingar i utrymmet anses vara inkomna till myndigheten. Användaren får stöd för att rätta till brister innan handlingen har sänts till myndigheten. Denna service kan kombineras med tekniska begränsningar som innebär att användaren inte kommer vidare för att skicka in handlingen utan att bristen har åtgärdats. Här blir det inte fråga om en bedömning av om en handling är att anse som inkommen enligt förvaltningslagen utan i vilken omfattning en myndighet ska vara tillgänglig för allmänheten.

Vissa allmänna skyldigheter följer av reglerna i 6 och 7 §§ FL om service och tillgänglighet. Enskildas kontakter med myndigheter ska förenklas så att kontakterna blir smidiga och enkla (6 § FL). Myndigheter ska vidare vara tillgängliga för allmänheten i så stor utsträckning som möjligt (7 §). Bestämmelsen är neutral i förhållande till digital förvaltning vilket innebär att tillgänglighetskravet för it-miljö inte längre är begränsat till vissa former av kontakter så som e-post eller digitala tjänster på webbplatser. Enskilda bör hjälpas till rätta så att de använder en lämplig kanal för att ge in en handling.

Frågor om automatiserade kontroller har berörts av regeringen i två lagstiftningsärenden.⁵⁰ Så som regeringen redovisat de där införda funktionerna är det

⁵⁰ Se regeringens proposition 2013/14:236 Elektronisk ansökan om lantmåteriförrättning där det anförts att det elektroniska förfarandet motverkar att sökanden av misstag fyller i ansökan fel eller utelämnar viktiga uppgifter, samtidigt som myndighetens behov av att göra kompletteringar minskar (s. 10). Det har vidare, i regeringens proposition 2014/15:10 Förbättringar av husavdragets fakturamodell, redovisats hur kontroller görs av att alla obligatoriska uppgifter är ifyllda och att även en viss formaliakontroll genomförs, samt att en begäran som saknar obligatoriska uppgifter inte kan lämnas innan den har kompletterats. Som exempel på fel, som helt kan undvikas om begäran om utbetalning



möjligt att utforma ett eget utrymme så att det inte går att komma vidare för att ge in en handling, om en brist konstateras vid den automatiserade service som ges i utrymmet och bristen inte har åtgärdats. Begränsningar kan göras eftersom den myndighet som tillhandahåller eget utrymme går utöver den miniminivå som gäller för serviceskyldigheten enligt 6 § FL.

Denna service ska emellertid avse procedurer som äger rum innan användaren har sänt iväg handlingen och utformas så att användarens berättigade behov av skydd tillgodoses. Avgörande är alltså inte den närmare utformningen av den service en myndighet erbjuder eller om förfarandet tar stopp i det egna utrymmet. Avgörande är om kontrollerna sker i det egna utrymmet eller först efter att handlingarna kommit till myndighetens mottagningsfunktion. Tar förfarandet stopp i utrymmet, där myndigheten inte får ta del av uppgifterna, är det inte fråga om ett beslut av myndigheten.

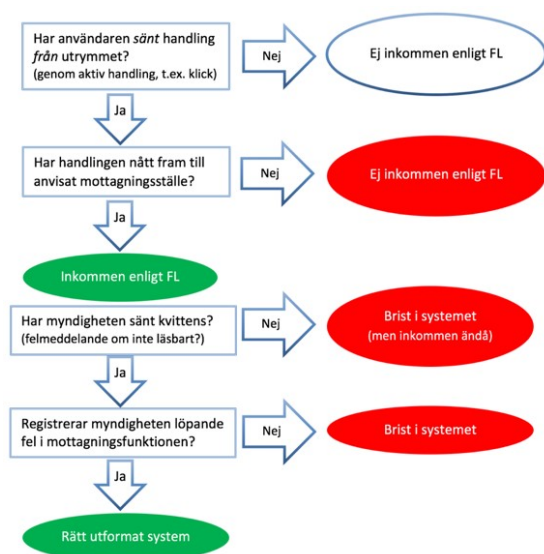
Genom att det t.ex. via e-post går att nå en annan mottagningsfunktion än den för servicetjänsten har användaren möjlighet att ge in en handling via en annan kanal.

Checklista för inkommande handlingar med mera:

- Vilken service ska myndigheten tillhandahålla genom eget utrymme?
- Finns det en tydlig punkt för att ge in handlingar så att det går att skilja mellan handlingar som finns endast i eget utrymme (t.ex. utkast) och de exemplar av färdigställda handlingar som sänts iväg till myndigheten?
- Anvisar myndigheten automatiserat en mottagningsfunktion som handlingar sändas till och finns det säkra funktioner för att registrera när en handling enligt 22 § FL har kommit in till myndigheten?
- Sänds kvittens från mottagningsfunktionen och underrättas avsändaren, inte bara när överföringen lyckades och handlingen är inkommen, utan även i de fall där ett meddelande inte har gått att läsa?
- Registrerar myndigheten händelser som tyder på att det finns något fel i mottagningsfunktionen och har myndigheten rutiner för att hantera material som nått myndigheten under sådana förhållanden?

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

kommer in via Skatteverkets e-tjänst, har angetts summeringsfel, avsaknad av obligatoriska uppgifter, avsaknad av undertecknande av utföraren och att betalningsdatum angetts som en senare dag än ansökningsdagen (s. 27).



3.4 Sekretess och tystnadsplikt

Den juridiska bedömningen av om det finns brister i sekretessen för eget utrymme blir, tillsammans med frågor om handlingsoffentlighet, ofta styrande för hur dessa funktioner ska utformas och införas. I eSams vägledning [Outsourcing 2.0 En vägledning om sekretess och dataskydd](#) finns en allmän genomgång av sekretessbestämmelsernas uppbyggnad och innebörd, sekretessbrytande bestämmelser samt överföring av sekretess och tystnadsplikt.

Här begränsas framställningen till de juridiska frågor som har uppfattats som oklara eller setts som hinder mot att använda eget utrymme till följd av att någon som sköter drift eller säkerhet i tjänsten skulle kunna få se uppgifter som finns i eget utrymme. Den som använder ett eget utrymme som en myndighet tillhandahåller behöver veta om det finns risk för att de uppgifter som hanteras där röjs för myndigheten eller någon annan. Här måste följande klarläggas.

3. Skyddas användaren av utrymmet mot insyn både från utomstående och från myndigheten och dess personal?
4. Kan en myndighet utkontraktera driften av eget utrymme utan att det leder till utlämnande av uppgifter till tjänsteleverantören i strid mot OSL eller risk för att tjänsteleverantören röjer uppgifter?
5. Vem ska göra sekretessprövningen? Kan den göras på förhand?
6. Får uppgifter lämnas ut till en tjänsteleverantör som lyder under en främmande rättsordning?



3.4.1 Utomstående ska inte ha insyn i eget utrymme

Ett löfte från en myndighet om att skydda uppgifter i ett eget utrymme mot insyn kan inte hindra ett utlämnande av en allmän handling.

Som tidigare nämnts blir innehållet i korrekt utformade utrymmen inte att betrakta som allmänna handlingar. En myndighet som tillhandahåller sådana utrymmen ska därför inte, till följd av en begäran om utlämnande av allmän handling, behöva ta del av uppgifter i utrymmen för att bedöma om de är offentliga eller sekretessbelagda.

Prövningen av den enskildes begäran kan begränsas till att konstatera att handlingarna inte är allmänna och därför inte lämnas ut. Något utlämnande med stöd av 6 kap. 4 eller 5 § OSL kommer inte heller i fråga.⁵¹

3.4.2 Personalen ska ha tystnadsplikt

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

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

Sköts it-driften av en *privaträttslig* leverantör, dvs. hos någon där tryckfrihetsförordningens och offentlighets- och sekretesslagens regler om handlingsoffentlighet och sekretess inte gäller, är det juridiskt möjligt att införa tystnadsplikt som sanktioneras genom avtal och arbetsrättslig reglering. Avtalsreglerad tystnadsplikt blir dessutom fullständig i den meningen att den inte behöver begränsas till vissa slag av uppgifter. Enligt den i avsnitten 2.6, 3.2.1 och 3.2.3 berörda propositionen 2019/20:201 Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter, har dessutom en ny lag om tystnadsplikt för privata tjänsteleverantörer. Lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgift syftar till att uppgifter från en myndighet som hanteras av en tjänsteleverantör ska få ett sekretesskydd som är likvärdigt med det som gäller när en annan myndighet tillhandahåller en motsvarande tjänst. Enligt propositionen bör en myndighet dock komplettera med en avtalsreglerad tystnadsplikt för sådana uppgifter som inte omfattas

⁵¹ Skulle det visa sig att en myndighet har utformat eget utrymme på fel sätt, så att handlingar som finns där har blivit allmänna, är det avgörande om uppgifterna skyddas av sekretess. Gäller absolut sekretess för uppgifter hos en myndighet är de skyddade medan motsatsen gäller om uppgifterna inte alls är sekretessreglerade. Eftersom uppgifter i ett eget utrymme inte hör till den tillhandahållande myndighetens ordinarie verksamhet kan det visa sig att en regel om sekretess för verksamhet som myndigheten bedriver inte omfattar uppgifter som finns där, jfr 40 kap. 5 § OSL och eSams vägledning [Outsourcing 2.0 En vägledning om sekretess och dataskydd](#).



av tystnadsplikten enligt den nya lagen (s. 13) och för de fall där brott mot tystnadsplikten enligt den nya lagen inte kan beivras (s. 20).

Tystnadsplikt för offentliga funktionärer regleras i stället i OSL. En sekretessbestämmelse begränsar nämligen inte bara allmänhetens rätt att ta del av uppgifter i allmänna handlingar. Den förbjuder också personal att röja en sekretessbelagd uppgift muntligen eller på något annat sätt (3 kap. 1 § OSL). Det är därför viktigt att klarlägga om sekretess gäller enligt OSL, i de fall it-driften sköts av personal hos en myndighet.⁵²

Alla typer av uppgifter omfattas inte av tystnadsplikt enligt OSL. Innehållet i eget utrymme behöver ändå skyddas mot att röjas av myndighetens personal. Eftersom eget utrymme ska vara utformat så att undantaget enligt 2 kap. 13 § TF blir tillämpligt (och därmed 40 kap. 5 § OSL) behöver myndigheten dock inte, vid en begäran om att få ut en allmän handling som finns i ett rätt utformat eget utrymme, ta del av innehållet för sin prövning.

Innehållet i eget utrymme behöver utformas så att personalen *inte kan* och – beträffande någon enstaka person med särskilt hög behörighet – *inte får* bereda sig tillgång till uppgifter i egna utrymmen. Bereder sig någon ändå olovligen tillgång till sådana uppgifter ska regler, avtal och tekniska begränsningar så långt möjligt utformas så att det kan dömas till ansvar om myndighetens personal missbrukar sin tillgång till data.

För egna utrymmen som avses användas för uppgifter som inte omfattas av en tystnadsplikt behöver särskilda åtgärder vidtas så att de som sköter driften inte råkar få syn på innehåll i egna utrymmen; jfr att en vaktmästare som har huvudnyckel till en lägenhet och går in för att stoppa ett vattenläckage får syn på och läser t.ex. ett utkast till en inlaga i ett ärende. När sådana begränsningar har införts återstår endast ett fåtal ”lovliga” fall där den som sköter driften av egna utrymmen utför en uppgift så som att rätta ett tekniskt fel eller att åtgärda en informationssäkerhetsrelaterad brist och då råkar få syn på en uppgift i ett eget utrymme. I så fall finns ingen avsikt att ta del av uppgiften.

Trots en förfrågan hos flera av de myndigheter som tillhandahåller egna utrymmen har inte ensam inte kunnat finna exempel på att information kommit till en befattningshavare

⁵² När det övervägs om egna utrymmen har utformats så att informationen där omfattas av undantag i grundlag från offentlighetsinsyn behöver det uppmärksammas att tystnadsplikten enligt OSL bara i vissa fall *har företräde* framför rätten att meddela och offentliggöra uppgifter. Detta kan närmare beskrivas så att en bestämmelse om sekretess ofta för med sig en begränsning även av yttrandefriheten enligt regeringsformen. Rätten att meddela och offentliggöra uppgifter har enligt huvudregeln företräde framför den tystnadsplikt som följer av en sekretessbestämmelse, men den har aldrig företräde framför den sekretess för handling som gäller enligt samma bestämmelse (se 1 kap. 1 § TF och 1 kap. 1 och 2 §§ yttrandefrihetsgrundlagen, i det följande ”YGL”, 7 kap. 3 § första stycket 2 och 5 § TF och 5 kap. 1 § första stycket och 3 § 2 YGL). – I andra fall kan det däremot vara tillåtet för en befattningshavare som administrerar utrymmen och har fått del av en uppgift som finns där att lämna uppgiften muntligen till en journalist eller att själv publicera den, trots att uppgiften är sekretessbelagd. Det är dock aldrig tillåtet att med stöd av meddelarfriheten lämna ut den allmänna handling som den sekretessbelagda uppgiften framgår av. Beträffande exemplen där sekretess gäller enligt 27 kap. 1 § eller 40 kap. 5 § OSL är meddelarfriheten helt inskränkt enligt 27 kap. 10 § och 40 kap. 8 § OSL.



kännedom på detta sätt. För fullständighetens skull och för att säkerställa att tillräckliga regler och tekniska skydd införs, bör dock den som ska tillhandahålla egna utrymmen överväga regleringen även i denna del (jfr SOU 2014:39).

3.4.3 En tystnadsplikt gäller normalt enligt lag

En tystnadsplikt som är absolut gäller enligt OSL för uppgift om en enskilds personliga eller ekonomiska förhållanden beträffande verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning. Bestämmelsen kompletteras av en regel om överföring av sekretess när en myndighet får en uppgift i sådan teknisk verksamhet som hos den utlämnande myndigheten är sekretessreglerad av hänsyn till ett allmänt intresse.

Enligt 40 kap. 5 § OSL gäller sekretess i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning för uppgift om en *enskilds personliga eller ekonomiska förhållanden*. Denna tystnadsplikt är absolut, vilket innebär att uppgifter som omfattas av sekretessen ska hemlighållas utan någon skadeprövning. Bestämmelsen, som inte längre är begränsad till personuppgifter (se [prop. 2016/17:198](#)), är av direkt relevans avseende skyddet för uppgifter i egna utrymmen. Absolut sekretess gäller där för alla uppgifter om enskilds personliga och ekonomiska förhållanden, dvs. även rörande bolag och enskilda näringsidkare, se vidare [Outsourcing 2.0](#) – en vägledning om sekretess och dataskydd.

Utkontraktering har också underlättats genom en bestämmelse i 11 kap. 4 a § OSL där följande föreskrivs: Får en myndighet i verksamhet för enbart teknisk bearbetning eller teknisk lagring för en annan myndighets räkning en uppgift som hos den senare myndigheten är sekretessreglerad av hänsyn till *ett allmänt intresse*, blir sekretessbestämmelsen tillämplig även hos den mottagande myndigheten.

Det skydd som aktualiseras när sekretessen överförs med stöd av bestämmelsen är en tystnadsplikt som ska gälla både i samband med digitala tjänster som en myndighet tillhandahåller åt en annan myndighet och vid en myndighets utkontraktering av it-drift till en annan myndighet. Bestämmelsen är tillämplig även på uppgifter som den mottagande myndigheten får av enskilda och från andra myndigheter än beställarmyndigheten för den senare myndighetens räkning. Den gäller emellertid inte om en primär sekretessbestämmelse till skydd för samma intresse redan är tillämplig på uppgifterna hos den mottagande myndigheten, se 11 kap. 8 § OSL (a.prop. s. 28).

Till detta kommer den i avsnitt 3.3.2 redovisade lagen (2020:914) om tystnadsplikt för privata tjänsteleverantörer.



3.4.4 Utlämnandefrågan — nationellt och internationellt

Flera invändningar har gjorts över tid mot att det skulle kunna förenas med reglerna om sekretess att utkontraktera driften av eget utrymme. Förutsättningarna har till stor del klarlagts. Vissa frågor utreds emellertid alltjämt.

Frågan om det är tillåtet att lämna ut uppgifter till en tjänsteleverantör har uppkommit som en följd av att myndigheter utkontrakterar driften av bl.a. eget utrymme och upphandlar molntjänster. Internationellt uppkommer även normkonflikter mellan vår rättsordning och en laglig rätt att få ut uppgifter som myndigheter i tredje land kan ha enligt sin rättsordning.⁵³

Frågor kan också uppstå om olika tolkningar av parternas avtal. Ett exempel är undantag i outsourcingkontrakt för det fall att ”annat följer av lag” och leverantören menar att detta villkor också skulle innefatta undantag enligt utländsk lag eller annan författning. Avtal av detta slag innehåller ofta även en prorogationsklausul som innebär att en tvist ska prövas av utländsk domstol.

I detta avsnitt redovisas de bedömningar eSam gjort av utlämnandefrågan, såväl nationellt som internationellt.

3.4.4.1 Myndigheten ska göra sekretessprövningen

En sekretessprövning måste göras av utkontrakterande myndighet innan uppgifter lämnas ut till tjänsteleverantören eller innan uppgifter som en myndighet förvarar hos en tjänsteleverantör lämnas ut därifrån. Denna prövning får inte överlåtas till någon utanför myndigheten.

Det är myndigheten som ska pröva om en uppgift får lämnas ut.⁵⁴ Myndigheten får inte utan stöd i lag eller förordning överlåta sekretessprövningen till någon annan.⁵⁵ Detta gäller även uppgifter som finns hos en tjänsteleverantör. Varken rätten till offentlighetsinsyn eller sekretessen får kringgås. Handläggningen av frågor om utlämnande av allmänna handlingar innefattar myndighetsutövning och sådana

⁵³ Med den *internationella utlämnandefrågan* menas här de juridiska komplikationer som uppkommer för en svensk myndighet om en leverantör av it-tjänster, utan en föregående sekretessprövning av den svenska myndigheten, *antingen* måste lämna uppgifter till en utländsk myndighet på grund av att leverantören i egenskap av juridisk person tillhör en koncern, där moderbolaget har sitt säte i ett land som har en lagstiftning vilken ger en myndighet i det landet rätt att direkt begära information från samtliga bolag i leverantörens koncern, oberoende av inom vilket territorium ett koncernbolag verkar,

eller har en rätt enligt parternas kontrakt att lämna uppgifter till en utländsk myndighet till följd av villkor i kontraktet om undantag från sekretess, eller lagval i kontraktet enligt vilket uppgifter får lämnas till en utländsk myndighet enligt den rättsordning parterna avtalat om.

⁵⁴ Om inte beslutsrätten är delegerad tillkommer sådan behörighet normalt en statlig myndighetschef, se 5 § myndighetsförordningen (2007:515) och för kommunala förvaltningar vederbörande nämnd, se 6 kap. 37 och 38 §§ samt 7 kap. 5 § kommunallagen (2017:725).

⁵⁵ Se 2 kap. 17 § andra stycket TF, 2016/17:JO1 s. 351 och JO:s beslut den 21 maj 2019, dnr 3053-2018.



förvaltningsuppgifter får enligt 12 kap. 4 § regeringsformen överlämnas till enskild endast med stöd av lag.

Om ett kontrakt med en tjänsteleverantör skulle föra med sig att myndigheten berövas möjligheten att själv utföra sekretessprövningen i vissa fall (exempelvis vid en begäran direkt hos tjänsteleverantören enligt utländsk rätt) strider redan tecknandet av kontraktet mot rättsordningen. Ett undantag från kravet på sekretessprövning kan inte heller grundas på en riskanalys eller en sannolikhetsbedömning av risk.⁵⁶

3.4.5 Sekretessprövningen kan inte göras på förhand

Utkontrakterande myndighet kan inte på förhand göra en sekretessprövning beträffande utlämnande till utländska myndigheter.

I 8 kap. 3 § OSL regleras sekretess i förhållande till utländska myndigheter. En svensk myndighet får inte lämna en uppgift till en utländsk myndighet utan att den svenska myndigheten först har gjort en prövning av att uppgiften i motsvarande fall skulle få lämnas ut till en svensk myndighet. Det måste dessutom enligt den utlämnande myndighetens prövning stå klart att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten, en bedömning som kräver ställningstaganden från fall till fall.

En sekretessprövning av myndigheten kan alltså inte göras på förhand beträffande kommande utlämnanden till en utländsk myndighet utan först när en enskild begäran kommit om ett visst utlämnande.

3.4.6 Røjande enligt OSL

Den rättsliga regleringen måste vara hållbar för att ett røjande inte ska föreligga. Sannolikhetsbedömningar av risker räcker inte.

Den bedömning eSams juridiska expertgrupp gjorde i ett rättsliga uttalande den 17 december 2015 om røjandebegreppet enligt OSL⁵⁷ förutsatte, dels att tjänsteleverantören enligt avtal med uppdragsgivaren inte får ta del av eller vidarebefordra de uppgifter som tillgängligörs för tjänsteleverantören, dels att omständigheterna i övrigt medför att det är osannolikt att detta ändå sker. Endast om båda dessa förutsättningar är uppfyllda har

⁵⁶ Visserligen kan ett utlämnande utan beslut av myndigheten ske när det finns en laga befogenhet, t.ex. att åklagare och polis får göra en husrannsakan följd av beslag. En sådan rätt måste dock följa av gällande svensk rätt, europarätten eller folkrätten. Den kan inte grundas på regler oförenliga med folkrätten.

⁵⁷ Där uttalades att om uppgifter görs tekniskt tillgängliga för en tjänsteleverantör som enligt avtalet inte får ta del av eller vidarebefordra uppgifterna och omständigheterna i övrigt medför att det är osannolikt att detta ändå sker, ska uppgifterna enligt expertgruppens bedömning inte anses som røjda i offentlighets- och sekretesslagens mening. — Uttalandet omfattade inte globala molntjänster.



expertgruppen bedömt att uppgifter som tillgängliggörs för en outsourcingleverantör inte behöver anses vara röjda i offentlighets- och sekretesslagens mening.

Här räcker det alltså inte med en sannolikhetsbedömning av risken för ett röjande. Först måste den rättsliga regleringen i parternas avtal vara hållbar och förenlig med rättsordningen för att myndigheten ska få teckna kontraktet. Offentliga funktionärer måste säkerställa att deras agerande på det allmännas vägnar har legal grund. Saknas sådan grund får agerandet inte ske.⁵⁸ Hit hör att det inte får finnas risk för röjande till följd av bindande skyldigheter för tjänsteleverantören enligt främmande rätt. Regleringen av röjandefrågan kan inte ryckas ur sitt sammanhang. Där föreskrivs bland annat att myndigheten måste göra en sekretessprövning innan ett utlämnande får äga rum (2 kap. 17 § andra stycket TF). Detta gäller även om myndigheten förvarar uppgifterna hos en tjänsteleverantör. Denna regel får inte kringgås.

Görs sekretessreglerade uppgifter tekniskt tillgängliga för en tjänsteleverantör som är bunden av regler i ett annat land, enligt vilka tjänsteleverantören kan bli skyldig att överlämna information till en utländsk myndighet, utan en föregående prövning av den svenska myndigheten och utan att internationell rättshjälp anlitas eller annan laglig grund enligt svensk rätt, får uppgifterna anses vara röjda. Sannolikhetsbedömningar av risker för röjande räcker inte.

Har kontrakt tecknats och tjänsteleverantören utlovat sekretess, trots att leverantören vet att löftet inte kan hållas, eller tolkar leverantören ett undantag i avtalet för fall där ”annat följer av lag” så att det skulle innefatta även undantag i främmande rättsordningar, kan bland annat en skadeståndstalan bli aktuell.⁵⁹

För de fall där den rättsliga regleringen är hållbar och ovan beskrivna internationella risker inte föreligger står eSam emellertid fast vid följande bedömning i det rättsliga uttalandet den 17 december 2015 av röjandebegreppet enligt OSL. Om uppgifter görs tekniskt tillgängliga för en tjänsteleverantör som enligt avtalet inte får ta del av eller vidarebefordra uppgifterna och omständigheterna i övrigt medför att det är osannolikt

⁵⁸ Bakgrunden var ett beslut av JO den 9 september 2014, dnr 3032-2011, där en tystnadsplikt för en tjänsteleverantör och dennes personal endast var avtalsreglerad och därmed inte straffsanktionerad. Detta betraktade JO som otillräckligt när särskilt skyddsvärda uppgifter behandlades av privat anställd personal som tog del av informationsinnehållet. För eSam uppkom frågan om samma bedömning måste göras vid t.ex. it-drift, där leverantören av tjänsten och dennes personal enligt avtal varken fick eller skulle ta del av uppgifterna. I syfte att uppnå ett praktiskt gångbart resultat fann eSams juridiska expertgrupp genom 2015 års uttalande en ”smal spång” för fortsatt utkontraktering, förutsatt att tjänsteleverantörens personal enligt avtal varken fick ta del av eller vidarebefordra uppgifterna och omständigheterna i övrigt medförde att det var osannolikt att detta ändå skulle ske. Uttalandet från år 2015 missförstods emellertid av många så att det skulle räcka med en sannolikhetsprövning, utan att först ha sett till att den rättsliga regleringen av parternas mellanhavande är hållbar från myndighetens perspektiv.

⁵⁹ Det kan visa sig att leverantörens agerande strider mot ”tro och heder” (33 § avtalslagen) eller att generalklausulen i 36 § avtalslagen kan tillämpas.



att detta ändå sker, ska uppgifterna inte anses som röjda i offentlighets- och sekretesslagens mening.

För detta talar också att en tystnadsplikt införts vid utkontraktering av teknisk bearbetning eller lagring av uppgifter, utan att regeringen funnit det nödvändigt att samtidigt införa en sekretessbrytande regel.

It-driftutredningen har emellertid nyligen presenterat en analys där delvis andra bedömningar har gjorts. Bland annat hävdar utredningen att ett röjande sker redan genom att digitala data lämnats till en leverantör av it-drift även om tjänsteleverantören inte kan ta del av informationsinnehållet till följd av kryptering som inte kan brytas (se vidare SOU 2021:1).

3.4.7 Legalitetsprincipen

En avtalsreglering varigenom svensk förvaltningsverksamhet ska bedömas enligt utländsk rätt eller rättskipning som rör sådan verksamhet överlämnas till utländsk domstol är inte förenlig med legalitetsprincipen.

Den offentliga makten ska enligt grundlag utövas under lagarna (1 kap. 1 § tredje stycket RF). Med ”lagarna” menas inte bara föreskrifter på lagnivå utan även andra författningar och sedvanerätt, dvs. gällande svensk rätt och EU-rätt.⁶⁰ Myndigheterna måste därför ha en normmässig förankring för all sin verksamhet, även om den inte tar sikte på beslutsfattande i klassisk mening. Förvaltningsuppgifter som en myndighet utkontrakterat måste alltså utföras i enlighet med svensk rätt och berörd europarätt, exempelvis när driften av det it-system där myndighetens ärendehandläggning äger rum drivs av en privat tjänsteleverantör.⁶¹ En svensk myndighet får inte genom lagval, när en förvaltningsuppgift överlämnas, acceptera att offentliga förvaltningsuppgifter ska utföras i enlighet med en främmande rättsordning.⁶²

I grundlag finns också regler om den dömande verksamheten (rättskipningen). Det är inte förenligt med principen om maktutövningens normbundenhet att en svensk myndighet genom avtal överlåter en rättskipningsuppgift, som annars skulle prövats av

⁶⁰ Vidare framgår det av förvaltningslagen (2017:900) att en myndighet endast får vidta åtgärder som har stöd i rättsordningen (se 1 § andra stycket och 5 § första stycket). För det absoluta flertalet myndigheter under regeringen följer detta även av 3 § myndighetsförordningen (2007:515) där det föreskrivs att myndighetens ledning ska ansvara för att verksamheten bedrivs enligt gällande rätt och de förpliktelser som följer av Sveriges medlemskap i EU.

⁶¹ Om utkontrakteringen inte innefattar förvaltningsuppgifter behöver den dock inte strida mot legalitetsprincipen, men en bedömning måste ändå alltid göras om det är förenligt med OSL, EU:s dataskyddsförordning och säkerhetsskyddslagstiftningen att ingå det aktuella avtalet.

⁶² Även om parternas kontrakt bara gäller mellan dem, medför ett sådant lagval konsekvenser för det allmänna och för medborgarna eftersom myndigheten inte längre kan kräva att få sina förvaltningsuppgifter utförda i enlighet med svensk rätt och tillämplig europarätt. Denna lagbundenhet gäller inte bara meddelande av beslut med ingripande verkningar, som innefattar ”maktutövning”, utan även faktiskt handlande (se prop. 2016/17:180 s. 58).



svensk domstol, till utländsk domstol, när den rättsliga prövningen kan bli avgörande för hur den svenska myndigheten, i den utkontrakterade funktionen, kan utföra sina offentlighetsreglerade uppgifter, exempelvis hur handlingar bevaras och gallras i enlighet med svenska arkivförfattningar.

Se vidare beträffande legalitet, avsnitt 3.7 nedan och avsnitt 2.8 i eSams publikation Lagringsytor – infrastruktur för it-drift och samverkan.

3.4.8 Exit-frågan

Vanligtvis är uppsägningstiderna korta. Frågan är i stället vilka alternativ som bör väljas och hur en exit kan genomföras.

Avgörande för svenska myndigheter som upptäcker att de tecknat kontrakt som har någon av de juridiska brister som beskrivits ovan blir vilka åtgärder de kan och bör vidta för att fortsättningsvis säkerställa en rättsenlig hantering. Kommer en myndighet fram till att samarbetet med leverantören måste avvecklas blir frågan vad som händer vid en s.k. exit.

Myndigheten måste återfå sina data och kunna använda dem med motsvarande funktionalitet, dvs. övergå till en annan tjänst eller sköta driften själv utan att drabbas av för höga kostnader, driftstopp eller andra olägenheter. Myndigheter behöver därför säkerställa en fungerande exit redan när en molntjänst upphandlas.⁶³

Checklista för sekretess och tystnadsplikt:

- Gäller tystnadsplikt för tjänstelevererande myndighets personal?
- Gäller tystnadsplikt för myndighetens eventuella underleverantörer?
- Är tystnadsplikten författningsreglerad och sanktionerad genom straffansvar eller kan en avtalsreglerad tystnadsplikt i förening med arbetsrättsligt ansvar och en skyldighet att betala skadestånd räcka?

⁶³ De juridiska aspekterna som detta aktualiserar har genomlysts redan år 2016 i en rapport av nätverket Cloud Sweden Legal och sammanfattats i publikationen Lov & Data (nr 2016-4), där följande behov av reglering har lyfts fram. **Format (portabilitet)**, att återfå data i ett format som är läsbart för myndigheten och möjligt att använda, samt rätt att begära ut annan information som kan behövas för att kunna använda återlämnad data, såsom loggdata, revisionsdata, accessdata, användardatabas och av kunden genererad metadata. **Tidpunkt och kostnad**, att kunna kräva ett återlämnande av data i princip när som helst under avtalstiden till rimlig kostnad. **Mottagare**, att ha rätt att anvisa att data ska återlämnas, helt eller delvis, till en tredje part. **Säkerhetskopiering/redundans och radering**, att säkerhetskopiering ska ske på ändamålsenligt sätt under uppdragstiden och att slutgiltig radering ska genomföras när uppdraget är slut. **Underleverantörer**, att även de ska omfattas av regler om exit. **Support**, att leverantören ska ställa resurser till förfogande vid en exit för att återföra data och bistå med assistans kring migrering. **Påtryckningsmedel**, att effektiva sådana ska finnas om molntjänstleverantören inte uppfyller sina åtaganden vid exit. **Lagstiftning**, att avtalet ska ta höjd för förändrad lagstiftning och tillåta att bestämmelserna om exit justeras i enlighet med den nya regleringen. **Ansvar**, att ansvaret för förlust av data ges särskild uppmärksamhet och särregleras i de fall det föreligger ett åtagande av leverantören att säkerhetskopiera eller lagra data och/eller upprätthålla redundanta system. **Uppsägningstid**, att inte ge leverantören rätt att avbryta/avsluta molntjänsten i förtid annat än vid mycket allvarliga avtalsbrott och att uppsägningstiden under andra förhållanden bör vara av sådan längd att kunden alltid har en reell möjlighet att återta sin data och ordna en alternativ lösning.



- Gäller sekretess enligt 40 kap. 5 § OSL för alla uppgifter i utrymmet eller aktualiseras även överföring av sekretess enligt 11 kap. 4 a § OSL?

3.5 Bevarande och gallring

Egna utrymmen ska vara utformade så att handlingar som finns där inte blir allmänna. Arkivförfattningarna blir därmed inte tillämpliga. Skulle ett fel i eller ett brottsligt angrepp mot ett utrymme leda till att handlingar som finns där blir allmänna behöver åtgärder vidtas för att handlingarna inte ska kunna lämnas ut. Handlingar som felaktigt blivit allmänna till följd av tekniska misstag eller brottsliga angrepp som rör eget utrymme kan normalt gallras.

En myndighet som tillhandahåller egna utrymmen behöver genom noggrant utformade regler och tekniska begränsningar se till att otillåten hantering av uppgifter i egna utrymmen motverkas.

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

Har en handling blivit allmän får gallring äga rum bara om åtgärden är tillåten enligt särskilda gallringsföreskrifter i lag eller förordning eller i enlighet med föreskrifter eller beslut av Riksarkivet.⁶⁴ För kommuner och landsting framgår det inte av arkivlagen vem som ska besluta om gallring vilket innebär att nämnderna, som verksamhetsansvariga och ansvariga för vården av sina handlingar, själva beslutar om gallring av sina handlingar, om inte fullmäktige beslutat att arkivmyndigheten ska ha detta ansvar.⁶⁵ Här kan också noteras att en allmän handling, enligt 5 kap. 1 § OSL, varken behöver registreras eller hållas ordnad om det är uppenbart att den är av ringa betydelse för myndighetens verksamhet och inte omfattas av sekretess.

Riksarkivet har utfärdat generella gallringsföreskrifter för handlingar av tillfällig eller ringa betydelse för myndighetens verksamhet. Enligt 7 § Riksarkivets föreskrifter och allmänna råd om gallring av handlingar av tillfällig eller ringa betydelse (RA-FS 1991:6;

⁶⁴ Se 10 § arkivlagen (1990:782) och 14 § arkivförordningen (1991:446). Handlingar som skickas från eget utrymme till myndighet behöver uppfylla Riksarkivets föreskrifter och allmänna råd om tekniska krav för elektroniska handlingar (RA-FS 2009:2).

⁶⁵ Se vidare Arkivlagen – En kommentar- U Geijer m.fl. , Norstedts gula bibl., 2013, s. 194.



ändrad genom RA-FS 1997:6) får sådan gallring äga rum endast under förutsättning att allmänhetens rätt till insyn inte åsidosätts och att handlingarna bedöms sakna värde för rättskipning, förvaltning och forskning. För kommuner och landsting gäller som framgått särskilda regler.

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

Vid teknisk bearbetning eller lagring i anslutning till digitala tjänster som tillhandahålls av myndigheter är det enskildas handlingar som berörs. När det gäller sådan privat information, som ofta sammanställs som ett led i framtagandet av handling som sedermera ska ges in till myndigheten, som hanteras av myndigheten uteslutande för den enskildes räkning, har regeringen ansett att det i stort helt saknas insynsintresse i de handlingar som lagras ([prop. 2016/17:198](#) s. 20). Enligt [Juridisk vägledning för verksamhetsutveckling](#) inom e-förvaltning 3.0 (avsnitt 9.8) kan omedelbar gallring tillgodose enskildas befogade förväntningar på att andra inte ska ges tillgång till visst material.⁶⁶

Skulle i något undantagsfall t.ex. ett tekniskt fel i eller ett brottsligt angrepp mot ett eget utrymme leda till att handlingar där har råkat bli allmänna behöver myndigheten vidta åtgärder för att skydda innehavaren. Eftersom eget utrymme tillhandahålls som användarens eget och särskilt har utformats för att ingen annan ska få ta del av det som finns där kan det enligt eSams bedömning antas att hinder normalt inte finns mot att myndigheten beslutar att gallring får göras av handlingar som råkat bli allmänna.⁶⁷

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

Begränsningar behöver således införas så att den tjänst en myndighet tillhandahåller faller inom ramen för myndighetens uppgifter. Vidare krävs begränsningar från

⁶⁶ Liknande frågor uppkommer om uppgifter görs tillgängliga för en myndighet i en hjälptjänst och när uppgifter samlas in av myndighet för att sammanställas innan de lämnas ut till eget utrymme.

⁶⁷ JO har inte funnit anledning att kritisera en myndighet som – med stöd av ett beslut om gallring av handlingar av tillfällig eller ringa betydelse – raderat ett otillåtet register över samtliga e-postmeddelanden som medarbetare inom myndigheten tagit emot och skickat under en viss tidsperiod (JO:s beslut den 2 Mars 2016, dnr. 6696-2014).



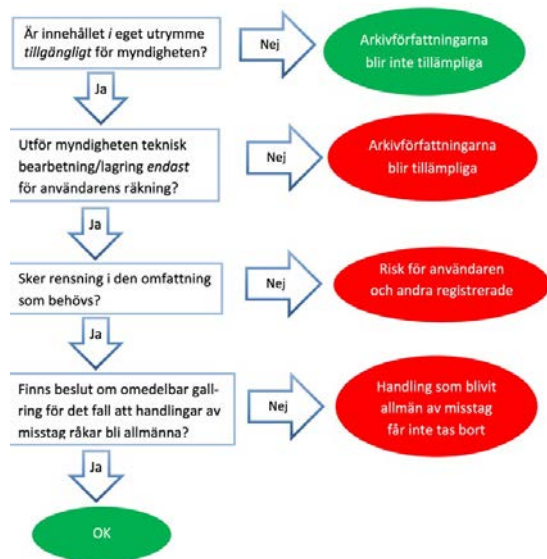
informationssäkerhetssynpunkt och för att personuppgifter inte ska behandlas längre än vad som är nödvändigt för ändamålet. Angivet ändamål blir här av avgörande betydelse för hur utrymmet ska få användas. En myndighet som tillhandahåller eget utrymme bör därför genom noggrant utformade tekniska begränsningar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

Checklista för bevarande och gallring:

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

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

Ref. 000001



Figur över bevarande och gallring

3.6 Skyddet för personuppgifter

En myndighet är normalt personuppgiftsansvarig för behandlingen av personuppgifter i eget utrymme. Om det framkommer att den enskilde behandlar personuppgifter i strid



med användarvillkor och andra instruktioner ska myndigheten skyndsamt ta ställning till om kontot ska stängas ned.

3.6.1 Vem är personuppgiftsansvarig?

Enligt artikel 4.7 dataskyddsförordningen är det den som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter som är personuppgiftsansvarig för behandlingen. Vem som bestämmer ändamål och medel ska avgöras utifrån faktiska omständigheter.⁶⁸ Personuppgiftsansvarig kan vara en fysisk eller juridisk person, en offentlig myndighet, institution eller annat organ. Medlemsstaterna kan fastställa i nationell rätt vem som är personuppgiftsansvarig. I Sverige regleras myndigheters personuppgiftsansvar ofta i en registerförfattning som gäller för det område av myndighetens personuppgiftsbehandling som registerförfattningen reglerar.

Frågan om i vilken mån myndigheten är personuppgiftsansvarig för de behandlingar av personuppgifter som utförs i eget utrymme har varit föremål för diskussion under flera år. Det finns än så länge inte någon vägledande dom på området. Det finns emellertid mycket som talar för att myndigheten som upplåter eget utrymme ensamt är personuppgiftsansvarig, särskilt när det är fysiska personer som innehar eget utrymme. Det är myndigheten som beslutar att ett eget utrymme ska inrättas och vilken utformning detta ska ha, vilka säkerhetsnivåer som ska gälla, vilka möjligheter som ska finnas för att inhämta uppgifter från och lämna ut uppgifter till andra myndigheter samt vem som ska svara för drift och förvaltning. Det är vidare myndigheten som ställer upp villkor för användningen av det egna utrymmet. Det är också myndigheten som har möjlighet att tillgodose de rättigheter som tillkommer den enskilde. Även dessa omständigheter innebär att det är myndigheten som regel bär personuppgiftsansvaret för den behandling av personuppgifter som äger rum i eget utrymme.⁶⁹

En sådan bedömning av personuppgiftsansvaret vid myndigheters behandling av personuppgifter vid utförande av sina uppgifter bidrar till tydlighet för de som berörs av personuppgiftsbehandlingen, och främjar på det sättet enskildas friheter och rättigheter och särskilt skyddet vid behandling av personuppgifter. Det blir förutsebart för den enskilde vem som ansvarar för behandlingen av personuppgifter när denne använder eget utrymme och vem den enskilde ska vända sig till för att begära sina rättigheter.

⁶⁸ Se Artikel 29-gruppens vägledning Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169), antagen den 16 februari 2010, s 8 där det framgår att "one should look at the specific processing operations in question and understand who determines them, by replying in a first stage to the questions 'why is this processing taking place? Who initiated it?'".

⁶⁹ Det finns några få avgöranden i svensk praxis där en domstol tagit ställning till frågan om personuppgiftsansvar för behandlingen av personuppgifter inom ramen för myndigheters digitala tjänster. Av störst relevans för denna utredning är Förvaltningsrätten i Stockholms avgörande om eHälsomyndighetens tjänst HälsaFörMig, se Förvaltningsrätten i Stockholms dom den 24 maj 2018 i mål 11458-17. Att myndigheten inte har haft möjlighet att råda över personuppgiftsbehandlingen har inte ansetts vara en omständighet som fräntar myndigheten personuppgiftsansvaret så länge som myndigheten beslutar om ändamål och medel, se Högsta förvaltningsdomstolens avgörande av den 5 juni 2012 i mål nr 4453-10 rörande en sms-tjänst för anmälan om sjukt barn som tillhandahölls av Försäkringskassan.



3.6.2 Vad innebär myndighetens personuppgiftsansvar?

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

1. En myndighet kan bara tillhandahålla eget utrymme för sådan behandling av personuppgifter som är tillåten enligt den dataskyddslagstiftning som gäller för myndigheten.⁷⁰ Myndighetens tekniska bearbetning och lagring av personuppgifterna i användarens utrymme skulle annars vara otillåten.
2. Myndigheten måste utforma utrymmet och instruktionerna till användaren så att det blir tydligt för vilka ändamål behandlingen av personuppgifter är tillåten samt vilka slags personuppgifter som är relevanta för ändamålet och därmed får behandlas i utrymmet.
3. Myndigheten måste tekniskt begränsa lagringstiden så att personuppgifter inte bevaras i utrymmet under längre tid än nödvändigt.
4. Myndigheten måste vidta lämpliga säkerhetsåtgärder för att skydda de uppgifter som behandlas i utrymmet. Detta gäller såväl funktioner för identifiering och kontroll av behörighet som åtgärder för att skydda utrymmet genom brandväggar, intrångsdetekteringssystem och liknande.
5. Myndigheten måste säkerställa att ingen otillåten överföring till tredje land görs avseende personuppgifter i eget utrymme, t.ex. genom användning av vissa s.k. molntjänster.
6. Systemet ska inte tillåta sökningar som visar i vilka användares utrymmen som en viss personuppgift förekommer. Om sådana sökmöjligheter finns måste användarna på förhand informeras om att s.k. registerutdrag kan komma att lämnas ut till registrerade som begär ett sådant.

⁷⁰ När en registerförfattning gäller för en myndighet som tillhandahåller eget utrymme behöver författningens tillämpningsområde övervägas. Myndigheten måste bedöma om registerförfattningen eller EU:s dataskyddsförordning ska tillämpas



De ovan beskrivna åtgärderna kan vidtas utan att myndigheten behöver ta del av innehållet i någon användares utrymme. Myndigheten kan därmed säkerställa en ansvarsfull personuppgiftsbehandling utan att utrymmets karaktär som ”eget” påverkas. Vidare ska myndigheten inte vidta några andra åtgärder med handlingarna i utrymmet än att tekniskt bearbeta och tekniskt lagra dem för användarens räkning. Myndighetens personuppgiftsansvar påverkar därmed inte den tidigare redovisade bedömningen att handlingar i ett korrekt utformat eget utrymme omfattas av undantaget i 2 kap. 13 § första stycket TF och därmed inte utgör allmänna handlingar.

3.6.3 Vilket ansvar har innehavaren av utrymmet?

Den enskilde har mycket begränsade möjligheter att påverka den behandling av personuppgifter som äger rum i eget utrymme, bortsett från sin egen faktiska användning av det egna utrymmet. Den enskilde har därtill mycket begränsade, om några, möjligheter att tillgodose sina egna och andras rättigheter. I den mån den enskilde använder utrymmet i strid med myndighetens instruktioner (såsom de framgår av exempelvis användarvillkor) och på ett sätt som utrymmet inte är avsett för, så bör det rimligen kunna medföra att den enskilde blir personuppgiftsansvarig för den behandlingen. Detta gäller under förutsättning att myndigheten utformat utrymmet på ett sätt som motverkar felaktig användning samt lämnat tydliga instruktioner till den enskilde och förvissat sig om att den enskilde tagit del av dessa.

Checklista för dataskydd:

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

3.7 Tillhandahållandet ska ingå i myndighets uppdrag

Serviceverksamhet genom eget utrymme ryms inom en myndighets uppdrag om verksamheten faller inom den yttre ram som anges vara myndighetens grundläggande



uppgifter och befogenheter. Aktiviteter helt vid sidan av det angivna uppdrag är däremot inte tillåtna.

I 1 kap. 1 § tredje stycket [regeringsformen](#) föreskrivs att ”Den offentliga makten utövas under lagarna.” Den offentliga förvaltningen präglas av normbundenhet.⁷¹ På lägre författningsnivå finns regler som ytterligare preciserar principen om lagbundenhet. Enligt 3 § [myndighetsförordningen](#) (2007:515) ska myndighetens ledning ansvara inför regeringen för verksamheten och se till att den bedrivs effektivt och enligt gällande rätt och de förpliktelser som följer av Sveriges medlemskap i EU. Av bestämmelserna i i [1 § andra stycket och 5 § första stycket FL](#) förvaltningslagen (2017:900; FL) följer också att myndigheter endast får vidta åtgärder som har stöd i rättsordningen. Enligt lagmotiven krävs som framgått att någon form av normmässig förankring måste finnas för all verksamhet som en myndighet bedriver, även för en myndighets faktiska handlande. Utvecklingen från en mer klassisk förvaltning mot en förvaltning med ökade inslag av informationsuppgifter och mera kundrelaterade aktiviteter, t.ex. i form av olika digitala självbetjäningstjänster, har inneburit ökade risker i detta avseende ([prop. 2016/17:180](#) s. 58 och s. 289).

En myndighets serviceverksamhet består inte bara av aktiviteter som direkt går att identifiera som utförande av uppgifter och befogenheter som framgår av författning, regleringsbrev eller särskilda regeringsbeslut. Verksamheten måste emellertid begränsas till vad som ligger inom myndighetens grundläggande uppgifter och befogenheter.⁷² Serviceverksamhet genom egna utrymmen för att förenkla för enskilda att t.ex. upprätta skattedeklaration eller att registrera företag får anses rymmas inom berörd myndighets uppdrag, utan särskild tillåtande reglering. Hjälpen faller inom den yttre ram som anges genom myndighetens grundläggande uppgifter och befogenheter.

Aktiviteter som ligger helt vid sidan av det i författning angivna uppdraget är däremot inte tillåtna. Det är inte alltid enkelt att avgöra var denna gräns går, men ska verksamhet som inte omfattas av uppdraget bedrivs av en myndighet krävs författningsändringar eller beslut av regeringen.⁷³ Så blir ofta fallet för användning av utrymmen för tjänster som mera liknar utkontraktering. Hur sådana funktioner etableras på ett rättsenligt sätt tas dock inte upp här utan i en vägledning om Lagringsytor - infrastruktur som möjliggör interoperabilitet och samverkan.

⁷¹ Strömberg, Håkan och Lundell, Bengt, Allmän förvaltningsrätt, 26 u., 2014, s. 16 f.

⁷² Se även [Juridisk vägledning för verksamhetsutveckling](#) inom e-förvaltning 3.0, s. 60 och [Digitalisera rätt](#) — en praktisk juridisk vägledning, avsnitt 2.2.

⁷³ Service som har direkt bäring på en viss ärendekategori som hör hemma inom myndighetens traditionella kärnverksamhet regleras normalt inte särskilt i lag eller förordning medan service av helt annat slag, t.ex. den som myndighet tillhandahåller genom mina meddelanden eller med avseende på elektronisk legitimering och underskrift, har stöd i uppdrag som följer av särskilda bestämmelser i förordning.



Vi har emellertid erfarit att det inte är ovanligt att en myndighet för säkerhets skull vill ha en författningsändring eller ett särskilt regeringsbeslut för varje enskild åtgärd, även när ordalydelsen i tillämpliga bestämmelser eller beslut och en rimlig tolkning därav ger vid handen att legalitetskravet redan uppfyllts. Beträds denna väg i alltför stor omfattning finns en risk för att motsvarande snåriga detaljregler uppkommer som i registerförfattningar. Det har samtidigt visat sig uppkomma situationer där regeringsbeslut i exempelvis regleringsbrev inte längre synes gälla för en verksamhet som etablerats. Verksamheten har emellertid fortsatt att bedrivas utan att det klarlagts om regeringsuppdraget alltjämt anses gälla för hanteringen.

3.8 Reglering av egna utrymmen

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

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

Eget utrymme har nu fått en omfattande spridning, med privaträttsliga handelsmönster och avtalskonstruktioner som förebild. Vad som tillhandahålls är dock endast en teknisk plattform med automatiserade funktioner för enskildas egen hantering av uppgifter. Dessa tjänster är begränsade till funktioner som lika gärna kan tillhandahållas genom en privaträttslig aktör. Inget förvaltningsärende har anhängiggjorts.

Så länge det inte finns någon offentligrättslig reglering av denna hantering finns enligt eSams bedömning inte hinder mot att införa regler genom avtal om användningen av eget utrymme. En myndighet som tillhandahåller eget utrymme bör således reglera dessa mellanhavanden med användare genom avtal. Tillhandahåller en myndighet under regeringen ett eget utrymme åt en annan myndighet under regeringen ingår de visserligen i samma juridiska person och avtal mellan dem kan inte prövas av domstol. Även sådan användning brukar emellertid regleras genom överenskommelser. Denna bedömning gäller även om myndigheten har utkontrakterat driften av den tjänst som myndigheten tillhandahåller åt enskilda.

Checklista för regler i avtal eller författning:



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

4. Praktisk utformning och användning

I detta kapitel ges exempel på hur eget utrymme och den digital infrastruktur som brukas i anknytning till sådana utrymmen har vidareutvecklats, delvis med stöd av ny rättspraxis och uttalanden i lagmotiv (se kap. 2 och 3).

4.1 Infrastruktur kring eget utrymme och programvaruföretag

En utgångspunkt för vår framställning är att kraven på eget utrymme ska uppfyllas så som de har beskrivits i avsnitt 2.3 och i rättspraxis. De följande exemplen tar istället sikte på hur ny digital infrastruktur har etablerats och kan tänkas utvecklas kring egna utrymmen för att underlätta individers och företags kontakter med det allmänna.



4.1.1 Digital årsredovisning — villkor godkänns i privat tjänst

I samarbete med Bokföringsnämnden, Skatteverket, Statistiska centralbyrån och Finansinspektionen har Bolagsverket etablerat en e-tjänst för företag där de kan ge in sin årsredovisning digitalt. För att bruka tjänsten för digital årsredovisning måste företaget ha ett bokföringsprogram, ett ekonomiprogram eller någon annan mjukvara som har anpassats för ändamålet. Företaget måste dessutom bruka den tjänst som Bolagsverket har etablerat. Något förenklat kan den infrastruktur som byggts upp beskrivas såhär.

1. Företag F tecknar avtal med en till infrastrukturen ansluten tjänsteleverantör (T) som tillhandahåller en redovisningstjänst för årsredovisning.
2. T hämtar grunduppgifter om F från Bolagsverket via ett API.
3. F upprättar årsredovisningen med hjälp av T:s tjänst. När den är upprättad ska F överföra en handling som återger innehållet i årsredovisningshandlingen till ett eget utrymme som Bolagsverket tilldelar F. I T:s tjänst visas därför för F villkoren för eget utrymme hos Bolagsverket och den information som ska lämnas enligt reglerna om dataskydd.
4. F accepterar villkoren och bekräftar att informationen lästs samt anger personnummer och e-postadress till styrelseledamot Z som ska skriva under ett fastställelseintyg beträffande årsredovisningen.
5. F laddar upp handlingarna till ett eget utrymme för F hos Bolagsverket.
6. Bolagsverket skickar en länk till Z för inloggning i det egna utrymmet.
7. Z loggar in i F:s eget utrymme, skriver under fastställelseintyget och skickar digitalt in handlingarna till Bolagsverkets mottagningsfunktion.
8. Z får en kvittens på att handlingarna har kommit in till Bolagsverket.
9. Bolagsverket handlägger det inkomna registreringsärendet.

Detta är ett exempel både på hur eget utrymme tillhandahålls för en organisation i stället för en individ och på hur en digital infrastruktur i allt större omfattning etableras av myndigheter kring egna utrymmen. Här sker dessutom en ny typ av egen delning genom att företaget överför uppgifter till ett eget utrymme hos Bolagsverket från förvar hos en privat tjänsteleverantör.

Bolagsverket har slutit avtal med ansluten tjänsteleverantör för att etablera den infrastruktur som krävs för dessa funktioner. Där ingår en funktion för att tjänsteleverantören via API ska kunna hämta viss kvalitetssäkrad information för att underlätta företagets arbete med årsredovisningen. Genom avtalet har Bolagsverket dessutom etablerat en funktion där företaget får ta del av och acceptera villkor för eget utrymme



och får erforderlig information innan uppgifterna överförs via API till ett eget utrymme. Därigenom har frågan om hur avtal med Bolagsverket ska finnas på plats innan uppladdning sker blivit löst, trots att företaget inte har besökt Bolagsverkets webbplats.⁷⁴ Till detta kommer att företag som så önskar automatiserat kan kontrollera sin upprättade årsredovisning i det egna utrymmet innan den ges in till Bolagsverket, om tjänsteleverantören har infört stöd för detta. I övrigt används de grundfunktioner som har beskrivs i avsnitt 2.5 utifrån de juridiska förutsättningar som redovisats i kap. 3.

4.1.2 Arbetsgivardeklaration – många roller, flera system kan ladda upp

Genom ändringar i skatteförfarandelagen (2011:1244) har en skyldighet införts för den som är registrerad som arbetsgivare att individuellt för varje anställd månadsvis i en arbetsgivardeklaration redovisa utbetalda ersättningar, avdragen skatt och arbetsgivaravgifter. För detta ändamål tillhandahåller Skatteverket en traditionell e-tjänst med eget utrymme där vissa uppgifter förifylls av verket. Skatteverket har också infört en tjänst där API:er används för funktioner som liknar dem Bolagsverket har för årsredovisningar. Arbetsgivare kan därmed skapa och ladda upp deklaraionsuppgifter med hjälp av sitt lönesystem. Följande exempel beskriver hur det går till:

Ref. 000001

⁷⁴ Beträffande dessa funktioner i tjänsten innehåller avtalet mellan Bolagsverket och tjänsteleverantören följande: Ansluten tjänsteleverantör ska tillhandahålla en funktion i redovisningstjänsten där Bolagsverket kan visa upp de villkor som gäller för att få använda Eget utrymme och lämna den information som krävs enligt reglerna om persondataskydd. Ansluten tjänsteleverantör ska också tillhandahålla en funktion för Användaren eller Ombudet där denne kan acceptera villkoren, bekräfta att denne tagit del av informationen och ladda upp Årsredovisningshandlingarna.



1. Arbetsgivaren A som har två kontor med många anställda ska upprätta sin månatliga arbetsgivardeklaration. Kontor 1 använder för sin personal Lönesystem 1 som ett löneprogramvaruföretag tillhandahåller medan Kontor 2 använder Lönesystem 2 som ett annat löneprogramvaruföretag tillhandahåller. Båda systemen är anslutna till Skatteverkets infrastruktur.
2. A:s personal vid Kontor 1 och Kontor 2 kan direkt i Lönesystem 1 och Lönesystem 2 (vid behov) hämta information via det API som Skatteverket tillhandahåller för arbetsgivardeklaration exempelvis när berörd individ är deklaraionsombud (exempelvis om deklaraionsdatum och vissa frågor kring A:s eget utrymme hos Skatteverket).
3. För den månad som gått sammanställer A i Lönesystem 1 och 2, genom personal vid respektive Kontor, de uppgifter för månadens deklaration.
4. Kontor 1 och Kontor 2 laddar därefter till A:s eget utrymme upp det underlag som sammanställts. Detta sker direkt från Lönesystemen via Skatteverkets API utan användargränssnitt hos verket. Identifiering av avsändaren sker genom e-legitimation eller servercertifikat för Lönesystemet.
5. I eget utrymme sker en automatiserad kontroll av underlaget och ett kontrollresultat skickas via API tillbaka till Lönesystem 1 och 2 där den som laddat upp materialet eller ett registreringsombud får se helheten.
6. Visade kontrollen inga fel skapas ett underlag för underskrift i A:s eget utrymme och en länk skickas till Z som är behörig företrädare för A.
7. Z loggar in hos Skatteverket, granskar utkastet till arbetsgivardeklaration och skriver under samt skickar till verkets mottagningsfunktion.
8. Mottagandet bekräftas med en kvittens via API till berörda Lönesystem.
9. Behörig personal hos A kan därefter i Lönesystemen, via Skatteverkets API, få information om ärendets gång.
10. Ytterligare roller möjliggör en flexibel åtkomst för olika aktörer som uppfyller det rättsliga förutsättningarna för att få åtkomst till uppgifter.

Även detta är ett exempel både på eget utrymme för en organisation och på hur en digital infrastruktur etableras av en myndighet kring egna utrymmen. Ett företag (arbetsgivaren) överför uppgifter till ett eget utrymme hos myndighet direkt från sitt lönesystem, på liknande sätt som för årsredovisningshandlingar. Här sker kommunikationen direkt via API mellan arbetsgivarens eget utrymme hos Skatteverket och en eller flera tjänster som programvaruföretag tillhandahåller åt arbetsgivaren. Tjänsterna har utformats så att arbetsgivarens personal eller ombud i olika roller kan använda funktioner i eget utrymme hos Skatteverket. Inloggningen kan också ske på olika sätt, med stöd av ett organisationscertifikat eller med vanlig e-legitimation via programvaruföretagets system men med Skatteverkets tjänst för inloggning till API för



eget utrymme. Först när deklARATIONEN är färdig loggar en behörig företrädare in, granskar, undertecknar och skickar den till verkets mottagningsfunktion.

För att reglera detta tecknar Skatteverket avtal (på motsvarande sätt som Bolagsverket i exemplet ovan) med de programvaruföretag som ansluter sig till infrastrukturen. I avtalet ställs nödvändiga juridiska och säkerhetsmässiga krav mellan parterna. Arbetsgivaren tecknar i sin tur avtal med programvaruföretaget om den tjänst arbetsgivaren använder. Där är skatteverket inte part. Bolagsverket ingår däremot [avtal](#) även med det företag som ger in en årsredovisning. Många individer, med olika roller och juridisk behörighet, kan agera med stöd av Skatteverkets API beroende på vilket led i hanteringen det är fråga om. I övrigt används även här de grundfunktioner som har beskrivs i avsnitt 2.5 utifrån de juridiska lösningar som redovisats i kap. 3.

4.1.3 Digital infrastruktur för återanvändning av uppgifter

Även här är det en utgångspunkt att de krav som beskrivits i avsnitt 2.3 och närmare utvecklats i rättspraxis ska uppfyllas beträffande eget utrymme och den befordran av meddelanden som äger rum. Följande exempel är istället inriktade på hur digital infrastruktur för återanvändning av uppgifter kan etableras för att företag och individer ska kunna ta tillvara att många uppgifter redan finns registrerade på ett tillförlitligt sätt.

För att företag inte ska behöva samla in och registrera samma uppgift flera gånger i sina kontakter med myndigheter har diskussioner visserligen förts kring något som kallats gemensamt eget utrymme. Tanken med ett gemensamt utrymme verkar vara att innehavaren av det ska vara en och densamma medan flera myndigheter i juridisk mening ska anses tillhandahålla utrymmet (medan driften av det sköts av en myndighet). Som redovisats i avsnitt 2.9 har eSam emellertid funnit ett en sådan inriktning för med sig ett antal juridiska utmaningar. Rättsordningen bygger på att varje myndighet själv har den juridiska rådgivningen över sina informationstillgångar och ”ensam” ansvarar för de funktioner som myndigheten tillhandahåller åt andra, jfr. den så kallade ansvarsprincipen. Arbete pågår därför istället med att utveckla en tjänst för *företagsprofil i eget utrymme*, se avsnitt 4.3.1.

För att kunna återanvända uppgifter som redan finns kvalitetssäkrade hos en eller flera myndigheter, i en individs eller ett företags kontakter med olika myndigheter, tillhandahåller Bolagsverket också en *sammansatt bastjänst för grundläggande uppgifter* (SSBTGU), se avsnitt 4.3.2.



4.1.4 Eget utrymme för företagsprofil — registrering för återanvändning

Ett arbete bedrivs inom Tillväxtverket, i samverkan med övriga myndigheter inom [verksam.se](https://www.verksam.se), för att etablera en s.k. företagsprofil i eget utrymme för individ (med visst personnummer). Där kan individen registrera vissa kategorier av uppgifter om ett företag. Samtidigt etablerar Tillväxtverket en infrastruktur för informationsutbyte så att den individ som innehar ett eget utrymme för företagsprofil mer eller mindre automatiserat ska kunna återanvända de i profilen registrerade uppgifterna i e-tjänster som andra myndigheter tillhandahåller. Denna återanvändning ska således kunna ske mellan individens eget utrymme för företagsprofil och de egna utrymmen som tilldelas hos annan myndighet, oberoende av för vilket företag uppgifter i profilen behövs. Endast de kategorier av uppgifter som det finns ett kartlagt behov av att återanvända och som Tillväxtverket valt ut ska kunna föras in i en företags profil. Följande exempel beskriver hur detta planeras gå till:

1. Företagare F loggar in på [verksam.se](https://www.verksam.se) med e-legitimation och begär eget utrymme för företagsprofil som lagras hos Tillväxtverket. Där visas för F villkor för eget utrymme och information enligt GDPR.
2. F accepterar villkoren, bekräftar att F tagit del av informationen och släpps in i ett eget utrymme för en viss företagsprofil.
3. När F registrerar uppgifter i olika guider på [verksam.se](https://www.verksam.se) uppdateras automatiserat även F:s företagsprofil.
4. F besöker vid senare tillfälle Myndighet M1 som efter inloggning med e-legitimation, tilldelar F ett eget utrymme åt företag AB där F är firmatecknare. F:s personnummer har styrkts genom e-legitimering. Uppgifter behövs från företagsprofilen för att F inte ska behöva skriva dem på nytt.
5. F återanvänder genom egen delning från sitt eget utrymme *för individ*, till det egna utrymme som M1 tilldelat AB *för organisation*, uppgifter från företagsprofilen i F:s eget utrymme *för individ*. Informationsutbytet sker via det API som Tillväxtverket tillhandahåller för infrastrukturen.
6. F återanvänder därefter i ett ärende hos en annan myndighet (M2), genom egen delning från sitt eget utrymme *för individ*, uppgifter till ett eget utrymme för individ som F tilldelats av M2.
7. F kan uppdatera sin företagsprofil efter hand när F ser behov av det. T reglerar och administrerar hanteringen så att den blir förenlig med de juridiska krav som gäller för den.



Detta är ett exempel både på eget utrymme *för individ* och på eget utrymme *för företag*, samt på hur en digital infrastruktur kan etableras där båda dessa typer av egna utrymmen används. Bland de grundfunktioner som redovisats i avsnitt 2.5 blir *egen delning* av särskild betydelse samtidigt som infrastrukturens *befordringsfunktion* gör det möjligt att överföra uppgifter mellan F:s eget utrymme för individ, där företagsprofilen finns, och F:s egna utrymmen för individ hos andra myndigheter respektive egna utrymmen för organisation som F nyttjar för organisationens räkning. Uppgifter i det utrymme för individ som T tillhandahåller åt F och uppgifter som befordras från därifrån och direkt hamnar i andra egna utrymmen för individ eller organisation blir inte allmän handling hos myndighet vid denna hantering. Skyddet mot insyn av andra än utrymmesinnehavare bibehålls därmed. Att F i vissa fall av informationsutbyte agerar för en juridisk person som tilldelats ett eget utrymme för organisation ändrar inte denna bedömning (se 2 kap. 13 och 14 §§ TF och 40 kap. 5 § OSL).

För att reglera en sådan användning tecknar Tillväxtverket avtal, dels med de myndigheter som ansluter sig till infrastrukturen för egen delning, dels med de individer som tilldelas eget utrymme för företagsprofil. I avtalen ställs nödvändiga juridiska och säkerhetsmässiga krav upp mellan parterna, bland annat så att den lagring som sker i form av en företagsprofil och det utbyte av uppgifter som äger rum begränsas för att hanteringen ska blir förenlig med bland annat reglerna om dataskydd. Legalitetsprincipen måste också upprätthållas genom reglering i författning eller uppdrag i exempelvis regleringsbrev så att de funktioner som Tillväxtverket erbjuder faller inom ramen för verkets uppdrag.

4.1.5 Sammansatta bastjänsten för grundläggande uppgifter (SSBTGU)

Infrastrukturen för vidareförmedling av grundläggande uppgifter om företag (SSBTGU) har två användningsområden. Den kan användas för att förifylla företagsuppgifter i eget utrymme i en e-tjänst eller för att hämta sådana uppgifter direkt till en myndighets verksamhetssystem. De uppgifter som återanvänds via SSBTGU hämtas från Bolagsverket, Skatteverket och SCB, kallade ”Producenter”. Producenterna tillhandahåller grundläggande uppgifter med stöd av [avtal](#) mellan dem och en aktör (Bolagsverket) som även agerar som ”Förmedlare” genom att tillhandahålla funktioner för befordran av begäran av uppgifter och svar mellan anslutna aktörer, och som ”Ledningsaktör” genom att handlägga och administrera avtal om anslutning till infrastrukturen och i övrigt förvalta den. Hanteringen går till så att Producenterna på begäran från användare söker



fram grundläggande uppgifter, beslutar om uppgifter ska lämnas ut och expedierar dem. Bolagsverket befordrar begäran, svar och utlämnade uppgifter mellan anslutna aktörer.

De myndigheter som har anslutit sig till infrastrukturen för att uppgifter ska lämnas ut kallas ”Konsumenter”. En Konsument kan ansluta sig till infrastrukturen för ”Direkt återanvändning”. Det innebär att den konsumerande myndigheten begär och får uppgifter direkt till sitt verksamhetssystem. Eget utrymme används därmed inte.

En konsumerande myndighet kan emellertid även använda infrastrukturen genom ”Indirekt återanvändning”. Det innebär att det är användare, som har tilldelats ett eget utrymme av den konsumerande myndigheten, som begär uppgifter via infrastrukturen och får dem utlämnade direkt till sitt eget utrymme och brukar dem där. En uppgift inkommer i dessa fall inte till konsumerande myndighet förrän användaren har skickat den från sitt eget utrymme till myndighetens mottagningsfunktion. Följande exempel visar hur en indirekt återanvändning kan gå till:

1. Användare A har loggat in hos myndighet M och tilldelas ett eget utrym. För att förenkla A:s arbete har M anslutit eget utrymme till SSBTGU.
2. A begär i sitt eget utrymme grundläggande uppgifter via SSBTGU.
3. Bolagsverket förmedlar via infrastrukturen A:s begäran till Bolagsverket, Skatteverket och SCB.
4. Bolagsverket, Skatteverket och SCB (Producenterna) prövar och beslutar automatiserat om uppgifterna ska lämnas ut eller om det finns hinder.
5. Efter att var och en av Producenterna automatiserat beslutat att bifalla A:s begäran expedierar de begärda uppgifter till A via SSBTGU. Uppgifterna överförs direkt till A:s eget utrymme utan att bli tillgängliga för M.
6. I A:s eget utrymme förs uppgifterna automatiserat in i berörds handlingar.
7. Resten av hanteringen i A:s eget utrymme berörs inte av SSBTGU.

Detta är ett exempel på hur enskildas användning av eget utrymme, för såväl individ som organisation, kan underlättas genom att grundläggande, kvalitetssäkrade uppgifter automatiserat lämnas ut till utrymmet och förfylls där. Det tydliggör samtidigt att digital infrastruktur redan finns i bruk för att återanvända uppgifter med stöd av sammansatta bastjänster.⁷⁵ Till använda grundfunktioner, som redovisats i avsnitt 2.5, hör

⁷⁵ Med bastjänst menas, som redan framgått av not 7, en lagringsyta för uppgifter med ett eller flera applikationsprogrammeringsgränssnitt, API:er, som möjliggör åtkomst till uppgifter som finns på lagringsytan.



infrastrukturens befordringsfunktion och de fråga- och svarsfunktioner som införts för automatiserade beslut i enlighet med HFD 2015 ref. 61 samt den egna hämtning som därmed äger rum. Skyddet mot insyn av andra än utrymmesinnehavare finns därmed kvar (se 2 kap. 6, 13 och 14 §§ TF och 40 kap. 5 § OSJ).

För att reglera detta tecknar Bolagsverket, Skatteverket och SCB avtal som Producenter om infrastrukturen. Även de myndigheter som vill använda dessas funktioner för återanvändning tecknar avtal, antingen för indirekt återanvändning i eget utrymme (så som i exemplet ovan) eller för direkt återanvändning i myndighetens verksamhetssystem. I avtalen ställs nödvändiga juridiska och säkerhetsmässiga krav på parterna. Legalitesprincipen måste upprätthållas genom reglering i författning eller uppdrag i exempelvis regleringsbrev så att de funktioner som Bolagsverket erbjuder faller inom ramen för myndigheten uppdrag.



Bilaga

Hos vem en tjänst finns

Följande sammanställningar ska konkretisera beskrivningen i avsnitt 2.8 genom exempel på hur en myndighetssamverkande kontaktpunkt kan indelas och avgränsas med hjälp av analogier från traditionell fysisk miljö.

Där kan gemensamma sidor i en webbportal liknas vid en trappuppgång i en byggnad medan de olika aktörernas webbsidor och tjänster kan betraktas som lokaler i samma byggnad. Vakten i kuren ersätts av identitetskontroller med e-legitimation. Dörren öppnas och tillträde ges till trappuppgången efter en lyckad identifiering.

1. <i>Portalen</i> ses som en <i>trappuppgång</i> med vaktkur	Jfr hur datatermgruppen hade definierat Portal som en webbsida som innehåller ingångar till ett större antal tjänster eller webbplatser (här webbsidor) med en gemensam nämnare (not 10)
2. <i>Ingångssida</i> ses som dörren till trappuppgången	Jfr hur datatermgruppen sett en analogi med ingången till ett hus
3. En eller flera <i>webbsidor</i> ses som en organisations lokal	Med webbsida menas den mängd information som användaren kan nå, utan att behöva gå vidare via en länk; jfr ett rum i en lokal
4. En <i>domänadress</i> avgränsar det som kan ses som huset	De webbsidor och tjänster som nås via portalen
5. En eller flera <i>webbadresser</i> går till den eller de webbsidor som hör till en lokal	En teckensträng identifierar en resurs i webben, här en webbsida som hör till portalen

eSam är ett medlemsdrivet program för samverkan mellan myndigheter och Sveriges Kommuner och Regioner (SKR) för att underlätta och påskynda digitaliseringen inom det offentliga. eSam bildades 2015 och en viktig uppgift är att ge ut vägledningar som skapar förutsättningar för att öka den digitala samverkan inom offentlig förvaltning.

Vägledningarna finns på esamverka.se

I eSam ingår Arbetsförmedlingen, Bolagsverket, Boverket, Centrala Studiestödsnämnden, Domstolsverket, eHälsomyndigheten, Försäkringskassan, Inspektionen för vård- och omsorg, Jordbruksverket, Kriminalvården, Kronofogdemyndigheten, Lantmäteriet, Migrationsverket, Naturvårdsverket, Patent- och registreringsverket, Pensionsmyndigheten, Polisen, Riksarkivet, Sida, Skatteverket, Skolverket, Sveriges Kommuner och Regioner, Statens servicecenter, Statens tjänstepensionsverk, Statistiska centralbyrån, Tillväxtverket, Trafikverket, Transportstyrelsen, Tullverket och Universitets- och högskolerådet

