

# Vägledning Lagringsytor - infrastruktur för it-drift vid myndighetssamverkan





## Innehåll

1. Inledning.....	4
2. Lagringsytor.....	5
2.1 Bagrund .....	5
2.2 En vidareutvecklad användning.....	5
2.3 Förutsättningar och utformning av lagringsytor.....	6
2.4 Grundfunktioner, olika typer av information och anskaffning av flera tjänster samtidigt	7
2.5 Den juridiska bedömningen .....	8
2.6 Krav på lagringsytor.....	9
2.7 Invändningar som bedömts i lagmotiv och praxis .....	12
2.8 Legalitetsprincipen .....	22
2.9 Rättslig grund för personuppgiftsbehandlingen .....	23
2.10 Dataskydd.....	24
2.11 Upphandlingsfrågor .....	26
3. Praktisk utformning och användning.....	27
3.1 Att tillhandahålla lagringsytor och infrastruktur .....	27
3.2 Exemplet studiestartstöd.....	28
3.3 Naturvårdsverket.....	30
3.4 Domstolarnas verksamhetsstöd .....	32



# 1. Inledning

I ett betänkande och flera vägledningar har E-delegationen och eSam redovisat sina juridiska bedömningar av den hantering som äger rum när myndigheter tillhandahåller eget utrymme.<sup>1</sup> Efter hand har en samsyn vuxit fram kring flera av dessa frågor. Numera har diskussionen istället kommit att handla om den digitala infrastruktur som etablerats kring egna utrymmen och de möjligheter den ger att kommunicera och i övrigt underlätta enskildas kontakter med det allmänna.

Parallellt med att en ny vägledning utarbetats inom eSam om ”Eget utrymme hos myndighet – en vidareutveckling” har även denna vägledning tagits fram om lagringsytor och den infrastruktur som hör till dessa ytor. Bakgrunden är att flera myndigheter börjat tillhandahålla tjänster åt andra myndigheter, undantagsvis även åt företag, där outsourcing av it-drift ingår (jfr software as a service, SaaS, och liknande). Dessa tjänster brukar i många fall nationell digital infrastruktur så att samverkan kan ske över myndighetsgränser.

Medan de flesta myndigheter behöver vägledning när det gäller eget utrymme (för individ och organisation) är den krets av myndigheter mera begränsad som har att ta ställning till hur lagringsytor och tillhörande infrastruktur bör utformas och införas. De verksamhetsutvecklare, arkitekter och jurister m.fl. som berörs är ofta inte heller desamma. Därför har eSam valt att ge ut, dels en vägledning beträffande eget utrymme och den vidareutveckling som ägt rum där, dels denna vägledning för lagringsytor och den infrastruktur som etablerats kring lagringsytor.

I den mån funktioner och rättsfrågor som uppkommer beträffande lagringsytor och tillhörande infrastruktur är desamma som för eget utrymme hänvisar vi i huvudsak till vägledningen ”Eget utrymme hos myndighet – en vidareutveckling”. Här redovisas främst det som är specifikt för lagringsytor.

Arbetet med att ta fram denna vägledning 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

<sup>1</sup> Se SOU 2014:39, E-delegationens Juridiska vägledning för verksamhetsutveckling inom e-förvaltningen och eSams publikationer, [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.



Wikström. Adjungerade ledamöter i expertgruppen är Eva Maria Broberg Lennartsson, Veronica Eckerby, Linn Kempe och Maria Sertcanli.

## 2. Lagringsytor

### 2.1 Bagrund

Genom eget utrymme har en allmän tillit kunnat skapas till digitala tjänster. Den utvecklingen kompletteras nu med lagringsytor som myndigheter tillhandahåller åt (andra) myndigheter eller företag och med tillhörande infrastruktur som myndigheter inför för kommunikation via lagringsytor.

Denna vägledning ska ses som ett stöd för att på ett rättsenligt sätt utveckla och införa lagringsytor och tillhörande infrastruktur.

### 2.2 En vidareutvecklad användning

I vägledningen Eget utrymme hos myndighet – en vidareutveckling (i det följande ”VL eget utrymme”), beskrivs de skillnader mellan eget utrymme och lagringsytor som gör det ändamålsenligt att skilja dem åt. Där förklaras vidare att det som myndigheter erbjuder till organisationer genom lagringsytor ofta är mera generellt till sin utformning och kan likna ren outsourcing av en funktion som myndigheten annars hade behövt utveckla själv (jfr software as a service, SaaS, och liknande). De grundläggande funktioner som tillhandahålls är visserligen ofta desamma som för eget utrymme, men de juridiska bedömningarna kan utfalla på annat sätt när en myndighet tillhandahåller funktioner åt andra myndigheter eller företag där de bedriver (delar av) sin förvaltningsverksamhet.

Till dessa funktioner hör också tjänster för att utbyta uppgifter mellan olika organ. Här brukas i många fall nationell digital infrastruktur så att interoperabilitet och samverkan över myndighetsgränser möjliggörs.

För att inte blanda ihop eget utrymme (för individ eller organisation) med tjänster som myndigheter erbjuder åt andra myndigheter för it-drift, använder vi begreppet lagringsyta för de ”utrymmen” som tillhandahålls åt andra myndigheter för it-drift. Det myndigheten tillhandahåller för att möjliggöra kommunikation med lagringsytor och övrig samverkan med anslutna aktörer kallar vi ”tillhörande infrastruktur”. Informationsutbytet sker där vanligtvis maskin till maskin via bastjänster till och från lagringsytor. Eget utrymme har däremot normalt ett användargränssnitt.



Vägledningen är i princip avgränsad till funktioner som en myndighet tillhandahåller åt andra myndigheter för att var och en av dem inte ska behöva bygga likadana eller likartade funktioner för exempelvis en viss kategori av ärenden. Till det som kan ingå i driftleveransen hör funktioner för eget utrymme, för att ta emot handlingar, för att handlägga de ärenden som anhängiggörs och för att expediera beslut eller andra handlingar till sökandena eller andra berörda. Vägledningen rör därmed också tillhörande infrastruktur för att kommunikation och informationsutbyte ska fungera. Respektive myndighet som anlitar den tjänstelevererande myndigheten avses ansvara gentemot enskilda eller myndigheter som brukar dessa funktioner för sina kontakter med den förstnämnda myndigheten (jfr software as a service, SaaS, och liknande).

Åtgärd	Funktion
En myndighet begär handlingar från en annan myndighet eller en enskild begär handlingar från annan, utan att detta sker genom direktåtkomst.	<b>Fråga- och svarsfunktion</b> 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	<b>Befordringsfunktion</b> 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	<b>Eget utrymme eller lagringsyta</b> 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.	<b>Mottagningsfunktion</b> jfr prop. 2016/17:180 s. 307, "på myndighetens server"
En myndighet sköter driften av nämnda funktioner åt en annan myndighet.	<b>It-drift</b> jfr TF 2:13
En myndighet hanterar information så att den blivit allmän handling och gallrar den genast för att skydda enskilda	<b>Omedelbar gallring</b> jfr TF 2:6
En innehavare av ett eget utrymme som från utrymmet begär uppgifter och får dem utlämnade direkt till sitt eget utrymme	<b>Egen hämtning</b> 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.	<b>Egen delning</b> jfr TF 2:13 och TF 2:14 st 1 p 1

Vägledningen omfattar däremot inte exempelvis funktioner för informationsförsörjning som myndigheter har i uppdrag att fullgöra inom särskilda områden och inte heller tillhandahållandet av öppna data.

## 2.3 Förutsättningar och utformning av lagringsytor

De funktioner som brukar finnas i eget utrymme har redovisats i avsnitt 2.3 i VL eget utrymme, där en sammanställning i [Juridisk vägledning för verksamhetsutveckling](#) inom e-förvaltning 3.0 har återgetts av krav som bör ställas på eget utrymme.



I kap. 3 VL eget utrymme har dessa krav därefter genomlysts med utgångspunkt i rättspraxis, uttalanden i lagmotiv och nya funktioner som har införts för egna utrymmen. För en närmare genomgång av dessa frågor hänvisas till VL eget utrymme, där även lagringsytor har berörts. Där har eSam redovisat bland annat följande.

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<sup>2</sup>, ge administrativt stöd och service åt domstolar<sup>3</sup>, utföra datorbearbetningar på uppdrag av myndigheter och enskilda samt tillhandahålla tjänster inom systemutveckling<sup>4</sup>, lagra och tillgängliggöra information i enlighet med vad berörda parter kommer överens om och bedriva uppdragsverksamhet som omfattar tekniskt handlägningsstöd i förrättningsprocessen<sup>5</sup>.

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.

## 2.4 Grundfunktioner, olika typer av information och anskaffning av flera tjänster samtidigt

I VL eget utrymme har beskrivits hur egna utrymmen och lagringsytor, tillsammans med tillhörande digital infrastruktur, har det gemensamt att de bygger på vissa (delar av) it-arkitekturer som används på ett likartat sätt. Dessa *grundfunktioner*, som redovisas i följande figur är normalt inte beroende av om det är ett eget utrymme eller en lagringsyta som erbjuds och inte heller av hur tillhörande infrastruktur närmare utformas.

En utgångspunkt för följande beskrivningar och exempel är att de lagringsytor som tillhandahålls och de överföringar av meddelanden som äger rum har utformats så att föreskrivna undantag i 2 kap. 13 och 14 §§ TF från handlingsoffentlighet blir tillämpliga och att erforderliga tekniska och administrativa begränsningar verkligen införs. En annan utgångspunkt är att det, även om vi från juridiska utgångspunkter betraktar förvaret av data som ett ”utrymme” eller en ”yta”, inte går att bortse från att dagens in-

<sup>2</sup> 1 § förordningen (2012:208) med instruktion för Statens servicecenter.

<sup>3</sup> 1 § förordningen (2007:1073) med instruktion för Domstolsverket

<sup>4</sup> 4 a § förordningen (2009:1174) med instruktion för Försäkringskassan

<sup>5</sup> 4 § andra stycket och 12 § 11 förordningen (2009:946) med instruktion för Lantmäteriet.



formationshantering och digitala kommunikation sker i it-system som har logiska gränser, sällan fysiska.

I VL eget utrymme beskrivs även de skilda miljöer som finns i en myndighets it-system – *verksamhetsmiljön* där den vanlige datoranvändaren befinner sig och där *nyttoinformation* finns i form av bl.a. ”originalhandlingar” respektive den *drift- och säkerhetsrelaterade miljön* där information finns som är av betydelse för driften och skyddet av systemen.

Dessutom redovisas i VL eget utrymme hur en tjänst ofta anskaffas tillsammans med andra tjänster och hur detta kan påverka de juridiska bedömningarna av dessa funktioner. Till lagringsytor 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.



Ref. 000001

Hela denna hantering behöver utformas så att gränserna mellan myndigheter eller andra organ inte bryts igenom och att individers och organisationers arbetsmaterial inte blir offentligt, se avsnitt 2.5 i VL eget utrymme.

## 2.5 Den juridiska bedömningen

Av kap. 3 i VL eget utrymme framgår att ett 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<sup>6</sup>,
- en handling som innehavaren har där omedelbart får gallras<sup>7</sup> 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 VL eget utrymme.

Därefter redovisas hur det som gäller för eget utrymme vanligtvis också gäller för lagringsytor. Det finns emellertid skillnader som brukar ha sin grund i att den som tillhandahåller en lagringsyta normalt tillhandahåller funktioner som blir en del av den andra myndighetens verksamhetssystem.

1. En handling som en myndighet för egen räkning förvarar på en lagringsyta hos en annan myndighet är allmän handling hos den första myndigheten om handlingen är att anse som inkommen eller upprättad där. Av 2 kap. 13 § TF följer emellertid att handlingarna undantas från offentlig-hetsinsyn hos den myndighet som tillhandahåller lagringsytan.
2. Enligt förvaltningslagen är en handling inkommen till den myndighet som har sina handlingar på en lagringsyta hos en annan myndighet om handlingen kommit till lagringsytan eller en mottagningsfunktion för den.
3. Legalitetsprincipen innebär att det normalt måste finnas ett tydligt uppdrag från regeringen för att en myndighet ska få tillhandahålla lagringsytor och tillhörande infrastruktur åt andra organ.
4. Bedömningen av frågor om dataskydd blir en annan när en myndighet inte tillhandahåller eget utrymme utan lagringsytor.

## 2.6 Krav på lagringsytor

Från dessa utgångspunkter bör följande krav ställas på en lagringsyta för att

1. handlingar på lagringsytan inte ska bli allmänna hos den myndighet som tillhandahåller ytan åt annan,
2. ett tillräckligt sekretesskydd ska finnas, och

<sup>6</sup> Jfr dock vad som beskrivs om teknisk personals åtgärder för att exempelvis upprätthålla en tillräcklig säkerhetsnivå eller hantera en incident.

<sup>7</sup> Handlingar som blivit allmänna hos en myndighet få dock gallras endast 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.





3. hanteringen ska följa förvaltningsrättsliga, dataskyddsrättsliga och straffrättsliga regler.

**Krav för att handlingar inte ska bli allmänna hos tjänstelevererande myndighet (2 kap. 13 § första stycket TF):**

1. Den myndighet som tillhandahåller lagringsytan 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 på lagringsytan för egen räkning eller annars förfogar över dem.
3. För att säkerställa skyddet ska dessutom endast viss teknisk personal hos en myndighet som tillhandahåller lagringsytor ha sådan behörighet att de kan bereda sig tillgång till uppgifter på lagringsytor.
4. Skulle personal råka läsa eller annars få del av information på lagringsytor, 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.

**Krav för att ett tillräckligt sekretesskydd ska finnas:**

1. Myndigheter som tillhandahåller lagringsytor bör se till att uppgifter som behandlas för en annan myndighets räkning hanteras så att de om-fattas av stark sekretess när den myndighet som utkontrakterat uppgiftshanteringen har en befogad förväntan att uppgifterna hanteras skyddade mot insyn, se 40 kap. 5 § offentlighets- och sekretesslag (2009:400), i det följande OSL, se även 11 kap. 4 a § OSL.<sup>8</sup>
2. En myndighet som tillhandahåller lagringsytor ska så långt det är möjligt ge tillträde för drift bara åt anställda och personal som på grund av uppdrag eller på annan liknande grund deltar i myndighetens verksamhet och därför omfattas av samma tystnadsplikt som anställda (2 kap. 1 § OSL).
3. Den myndighet som innehar lagringsytan bör vid tillträde till ytan identifieras på ett säkert sätt med serverlegitimation eller med stöd av en e-legitimation med

---

<sup>8</sup> I särskilda fall kan dock omedelbar gallring, när sådan får ske, ge ett tillräckligt skydd.



tillitsnivå 3 eller högre om det är en viss användare som begär tillträde. Är det en användare som begär tillträde<sup>9</sup> bör dennes behörighet också kontrolleras.

4. It-driftutredningen har 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).

#### **Krav från förvaltnings-, straff- och dataskyddsrättsliga utgångspunkter:**

1. Funktionerna ska utformas så att handlingar på en lagringsyta inte blir inkomna i förvaltningsrättslig mening hos den myndighet som tillhandahåller lagringsytan.<sup>10</sup>
2. Den myndighet som tillhandahåller lagringsytan ska agera i egenskap av personuppgiftsbiträde för den myndighet som nyttjar ytan.
3. Den myndighet som tillhandahåller lagringsytor ska förbjuda sin personal att läsa innehåll i sådana ytor.
4. Den myndighet som tillhandahåller lagringsytor bör ges rätt att gallra nyttoinformation som oavsiktligt blivit allmän handling.
5. Funktionerna får inte utformas så att de leder till övervakning eller kartläggning av enskildas personliga förhållanden eller andra liknande intrång i enskilds personliga integritet (prop. 2016/17:198 s. 24).
6. Det behöver finnas tydlig information om att e-legitimationer inte får missbrukas för att bereda tillträde för annan än den person som anges i legitimationshandlingen.<sup>11</sup>
7. Identifiering och behörighetskontroll ska utföras på ett säkert sätt.
8. Loggning ska ske så att incidenter kan utredas.

---

<sup>9</sup> Se beträffande denna hantering eSams publikation Juridisk vägledning för införande av [e-legitimering och e-underskrifter](#) 1.1.

<sup>10</sup> 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?](#)

<sup>11</sup> Se eSams rättsliga uttalande den 24 april 2017 [Missbruk av e-legitimation](#).



## 2.7 Invändningar som bedömts i lagmotiv och praxis

Samma invändningar som har gjorts över tid, mot att eget utrymme lagligen kan införas, kan förväntas beträffande lagringsytor. Efter hand har det dock klarlagts att ett undantag från handlingsoffentlighet finns när hanteringen har utformats på ett ändamålsenligt sätt.

Här redovisas den analys som presenterats i avsnitt 3.2.3 i VL eget utrymme efter att ha anpassats till de förutsättningar som gäller för lagringsytor.<sup>12</sup>

### **Den myndighet som tillhandahåller lagringsytor 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 lagringsytor får inte ta del av de handlingar som finns på dessa ytor. Handlingarna finns där endast som ett led i teknisk bearbetning och lagring för innehavaren av lagringsytan. Det innebär att

1. uppgifter som finns på lagringsyta inte i någon del får användas för den tjänstelevererande myndighetens egen räkning (HDF 2011 ref.52) och
2. tjänstelevererande myndighet, såväl administrativt som tekniskt, ska ha begränsat den egna personalens tillgång till de uppgifter som finns på tillhandahållna lagringsytor, så att de inte blir tillgängliga i läsbart skick för den egna personalen. De ska bara kunna ta del av drifts- och säkerhetsrelaterad information, inte nyttoinformation ([HFD 2018 ref. 48](#)).<sup>13</sup>

I lagmotiv har också uttalats att undantagen från offentlighet hos den myndighet som endast har en teknisk uppgift i sammanhanget ska gälla även för det fall att myndigheten som ett led i den tekniska bearbetningen för annans räkning har lov att överföra upptagningen i läsbar form (prop. 1975/76:160 s. 87). Regeringen har samtidigt anförts 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

<sup>12</sup> För en mera fullständig genomgång i vissa delar hänvisas till VL eget utrymme.

<sup>13</sup> Se vidare avsnitt 3.2.3 i eSams publikation "Eget utrymme hos myndig – en vidareutveckling.



ska kunna utföra sina arbetsuppgifter som ett led i den tekniska bearbetningen eller tekniska lagringen (prop. 2019/20:201 s. 23). För lagringsytor gäller dessa begränsningar på samma sätt som för eget utrymme.

Redan innan en lagringsyta tas i bruk bör de berörda myndigheterna ha kommit överens om hur de ska förfara, för den händelse hanteringen fallerar så att en handling på en lagringsyta blir allmän hos tjänstelevererande myndighet, exempelvis till följd av brott. En juridisk grund bör ha etablerats på förhand så att omedelbar gallring ska kunna ske hos den tjänstelevererande myndigheten för att minimera de skador eller andra olägenheter som en sådan oväntad, icke förutsedd händelse skulle inträffa.

### **Teknisk personal kan råka få se nyttoinformation**

För att tjänstelevererande myndigheter ska kunna sköta it-system även när de drabbas av tekniska fel eller angrepp måste några enstaka befattningshavare ha sådan åtkomst 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. Har en teknisk befattningshavare därvid råkat ta del av en uppgift gäller normalt en tystnadsplikt för denne. En förutsättning är dock att arbetet utförs i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning, dvs. inom området för 2 kap. 13 § första stycket TF<sup>14</sup>.

I [HFD 2018 ref. 48](#) prövade Högsta förvaltningsdomstolen 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. Domstolen fann att så inte var fallet när det saknades administrativa och tekniska begränsningar för myndigheten att ta del av uppgifterna i läsbart skick. Berörda handlingar hade inte avskilts från myndighetens verksamhetssystem och de hade dessutom använts för den tjänstelevererande myndighetens egen räkning. Här tog Högsta förvaltningsdomstolen 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.

Beträffande uppgifter i eget utrymme som avskilts från myndighetens verksamhetssystem, har Kammarrätten i Stockholm i en dom den 26 oktober 2015 ([mål nr.](#)

<sup>14</sup> 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.



[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. Detsamma gäller för lagringsytor. Samma bedömning har också gjorts av kammarrätten i Jönköping i en dom den 5 mars 2020 ([mål nr 3610-19](#), ej prövningstillstånd, den s.k. VERA-domen), där det prövades om tekniska och administrativa begränsningar som införts var sådana som avses i [HFD 2018 ref. 48](#). Av redovisningen i kammarrättens dom framgick beträffande VERA att

- informationen är logiskt avgränsad,
- det föreligger både tekniska och administrativa begränsningar,
- endast vissa medarbetare tilldelades sådan teknisk behörighet (s.k. central behörighet) att de kunde få teknisk åtkomst till handlingarna,
- dessa medarbetare är föremål för den administrativa begränsningen att befattningshavaren måste få ett medgivande från den myndighet som nyttjar tjänsten, och
- medarbetaren dessutom (efter att ha fått myndighetens medgivande) genom en knapptryckning behövde tilldelas sig själv faktisk behörighet att komma åt den andra myndighetens handlingar för att det skulle bli tillgängliga för denne i läsbar form.

Enligt Kammarrättens bedömning var det inte 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 alltså att dessa begränsningar var tillräckliga för att 2 kap. 13 § första stycket TF och 40 kap. 5 § OSL ska vara tillämpliga.

Denna bedömning vinner stöd av de ovan redovisade uttalandena i regeringens proposition 2019/20:201 Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter (s. 22-23). eSam delar denna bedömning och vill betona vikten av att tekniska och administrativa be-gränsningar införs 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](#). Följande rättsliga risker bör emellertid beaktas;

- om de tekniska och administrativa begränsningar som införs för lag-ringsytor inte är sådana som sägs i [HFD 2018 ref. 48](#), dvs. att det saknas administrativa och tekniska begränsningar att ta del av uppgifterna i läsbart skick,
- om de inte utformats så att förfoganderätten över nyttoinformationen är kvar hos den som anlitat tjänstelevererade myndighet, eller
- om tjänstelevererande myndighet inte har juridisk möjlighet att omedelbart undanröja en icke avsedd tillgång till kundmyndighetens uppgifter när angrepp eller andra fallissemang leder till att uppgifter sprids felaktigt.

### Handlingar i olika utrymmen bedöms var för sig

Handlingar som finns på en lagringsyta respektive i myndighetens verksamhetssystem bedöms var för sig från offentlighets- och sekretessynpunkt.

Regeringen använde sig av begreppet eget utrymme i ett 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<sup>15</sup>. Myndigheter tillhandahåller som framgått även lagringsytor som uppfyller dessa krav. Denna bedömning vinner stöd av regeringens uttalanden i proposition 2019/20:201 Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter (s. 22-23). Där har regeringen förklarat 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 på en lagringsyta eller i ett eget utrymme (utan att vara allmän handling där), och i en myndighets verksamhetssystem (som allmän handling), efter att en färdig handling skickats till myndighetens funktion för att ta emot inkommande elektroniska handlingar. På samma sätt kan en

<sup>15</sup> Se prop. 2016/17:198 s. 7, s. 16, s. 19 och s. 20. 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.



handling som bevaras (i ett exemplar) i myndighetens verksamhetssystem lämnas till en lag-ringsyta eller ett eget utrymme hos en annan myndighet eller sändas via Min myndighetspost till annan (i ett annat exemplar). Dessa olika exemplar av handlingar ska bedömas var för sig från offentlighets- och sekretesssynpunkt. Detta gäller oberoende av om handlingar med samma innehåll finns i såväl lagringsytor eller egna utrymmen som i verksamhetssystem etc. Dessa olika exemplar av en handling ska bedömas var för sig.<sup>16</sup> 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 lagringsytor behöver alltså utforma uppgiftshanteringen så att det tydligt går att skilja mellan exemplar av en e-handling som finns på en lagringsyta eller i en mottagningsfunktion för lagringsytan, respektive i ett verksamhetssystem hos myndigheten eller i en mottagningsfunktion där myndigheten tar emot handlingar för egen räkning.<sup>17</sup> Det ska dessutom tydligt gå att skilja drift- och säkerhetsrelaterad information från nyttoinformation i dessa miljöer. Detta blir av särskild betydelse när en myndighet, så som beskrivits i avsnitt 2.4, 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).

### Gränserna måste upprätthållas även vid informationsutbyte

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

<sup>16</sup> 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 sekretesssynpunkt och inte sammanblandas med användarens nyttoinformation i eget utrymme.

<sup>17</sup> Se eSams publikationer [Digitalisera rätt](#) — en praktisk juridisk vägledning, avsnitt 3.5





Handlingar kan utbytas till, från eller mellan lagringsytor eller till eller från 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 informationsutbytet utformas så att uppgifter blir tillgängliga för ”fel” aktör och att gränserna mellan berörda aktörer därmed bryts igenom.<sup>18</sup> 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 be-handling 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 lagringsytor.

- Rättsliga risker - att hantering utformas så att direktåtkomst uppkommer och att de uppgifter som hanteras för annan myndighet an-ses expedierade av denna myndighet och inkomna hos tjänsteleverantören utan att något undantag från handlingsoffentlighet gäller.

<sup>18</sup> 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.





- 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).

### 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.). Enligt [HFD 2019 ref. 29](#) är detta undantag från allmän handling inte tillämpligt på en av Kriminalvården granskad och kvarhållen försändelse till en intagen eftersom den befordran som därvid 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 gemenskaps-formgivning. Regeringen uttalade där 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.<sup>19</sup>

<sup>19</sup> Regeringen anförde vidare följande: Patent- och registreringsverkets befattning med de handlingar som skall vidarebefordras till byrån i Alicante kan inte jämföras med värdmyndigheters 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).



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.

### Hjälpjänster (support)

Sätts de grundfunktioner som beskrivits i avsnitt 2.4 samman på ett ändamålsenligt sätt kan information på en lagringsyta lämnas ut till en hjälpjänst genom en fråga- och svarstjänst. De exemplar av handlingar som finns kvar på lagringsytan omfattas därmed alltså av undantaget i 2 kap. 13 § första stycket TF från offentlighetsinsyn. Utlämnade handlingar blir allmänna.

Myndigheter som tillhandahåller lagringsytor får som framgått inte ta del av eller annars använda sig av 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 på en lagringsyta. Regeringen har uttalat att en myndighets tillhandahållande av hjälpjänster till enskilda har en annan karaktär än den digitala tjänst som hjälpjännen avser. De handlingar som kan uppstå i samband med tillhandahållandet av en hjälpjänst förvaras inte endast som led i teknisk bearbetning eller teknisk lagring för annans räkning. Även om tillhandahållandet av en hjälpjänst kan innefatta moment av teknisk bearbetning eller lagring kan det inte enbart anses utgöra sådan verksamhet.<sup>20</sup>

I [Juridisk vägledning för verksamhetsutveckling inom e-förvaltning 3.0](#) (avsnitt 8.1) har eSam beskrivit de olika typer av hjälpjänster 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 genom att den raderas.

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 hjälpjännen. Enligt vägledningen skulle utrymmet därefter avslutas på grund av att materialet i utrymmet sades bli allmän handling. Ett nytt (skyddat) eget

<sup>20</sup> 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).



utrymme skulle därefter kunna skapas för innehavaren. Samma funktioner för att ge hjälp skulle kunna införas för lagringsytor.

Frågan är emellertid om denna försiktiga bedömning är korrekt. Sätts de grundfunktioner (pusselbitar) som beskrivits i avsnitt 2.4 samman på ett ändamålsenligt sätt kan information i ett eget utrymme eller en lagringsyta lämnas ut genom en fråga- och svarstjänst. Den som ger hjälp får därmed inte direktåtkomst till utrymmet utan det är nya exemplar av handlingarna som förvaras i den hjälpgivande myndighetens verksamhetssystem för hjälptjänsten. Innehavaren av utrymmet förfogar alltjämt ensam över den information som finns på lagringsytan och bestämmer ensam över vad som ska lämnas ut via fråga- och svarstjänsten. De exemplar av handlingar som finns kvar på lagringsytan och de som överförts från ytan via en befordringsfunktion och nått verksamhetssystemet hos en myndighet som ger hjälp ska bedömas var för sig från offentlighets- och sekretessynpunkt.

Lagringsytan förblir därmed intakt från offentlighets- och sekretessynpunkt genom att undantaget i 2 kap. 13 § första stycket TF alltjämt är tillämpligt på de exemplar av handlingar som finns på lagringsytan. 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 lagringsutrymmen. 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 efterfrågad hjälp utan att tjänsteleverantörens befattningshavare får tillgång till lagringsytan.<sup>21</sup>

Genom att sätta samman de grundfunktioner som beskrivits i avsnitt 2.4 på ett ändamålsenligt sätt kan således information på en lagringsyta lämnas ut till en hjälptjänst genom en fråga- och svarstjänst. De exemplar av handlingar som finns kvar på lagringsytan omfattas därmed alltjämt av undantaget i 2 kap. 13 § första stycket TF från offentlighetsinsyn.

---

<sup>21</sup> 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.



- Rättsliga risker - att hantering utformas så att direktåtkomst upp-kommer och att uppgifter på lagringsytor 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 be-dömt i LEFI onlinemålet samt att annan åtkomst inte ges.
- Hur myndigheter kan förfara om en risk förverkligas - gallra omedelbart uppgifter efter att kundens tillgång till uppgifterna har säkrats (juridisk grund för detta behöver säkerställas på förhand).

### **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 används. Sådan information behövs ofta även för statistiska ändamål eller för att fördela kostnader mellan de aktörer 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 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). Samma bedömningar får anses gälla för lagringsytor.

En likartad bedömning har gjorts av Kammarrätten i Jönköping som, beträffande domstolars data hos Domstolsverket, uttalat att varje del av systemet och den information den delen innehåller ska 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 läsbar skick blev allmänna handlingar hos Domstolsverket ([mål nr 3610-19](#), 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. Detta behov blir särskilt tydligt när en myndighet, så som beskrivits i avsnitt 2.4, anskaffar flera funktioner från en och samma leverantör. De rättsliga risker och behov av åtgärder som uppkommer är desamma som i föregående avsnitt.



För att en myndighet ska få tillhandahålla lagringsytor måste detta falla inom ramen för myndighetens uppdrag. Aktiviteter helt vid sidan av myndighetens uppdrag är inte tillåtna.

Den offentliga makten ska, som närmare utvecklats i avsnitt 3.7 i VL eget utrymme, utövas under lagarna.<sup>22</sup> Detta gäller även när offentlig verksamhet digitaliseras.<sup>23</sup> Regeringen lämnar uppdrag till förvaltningen på olika sätt, exempelvis genom allmänna bestämmelser i lag eller detaljerade regler i speciallagstiftning. Det sker också genom allmänna eller särskilda bestämmelser i myndighetens instruktion eller i annan förordning som regeringen har beslutat. Legalitetskravet kan dessutom uppfyllas genom ett förvaltningsbeslut av regeringen, t.ex. när åtgärden ska utföras enligt myndighetens regleringsbrev.<sup>24</sup> Efter att kravet på legalitet införts i FL har frågan blivit mera uppmärksammat.<sup>25</sup> Föreskrifter som gäller för ett stort antal myndigheters insamling av uppgifter har dessutom införts i förordningen (2018:1264) om digitalt inhämtande av uppgifter från företag, som kan ge ett kompletterande stöd för tillkommande funktioner.

Serviceverksamhet genom egna utrymmen eller fråga- och svarstjänster för att underlätta kontakter med och uppgiftslämnande till den myndighet som handlägger berörda ärenden 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 de i författning eller genom regeringsbeslut angivna uppdragen är däremot inte tillåtna. Det är inte alltid enkelt att avgöra var denna gräns går, men ska verksamhet som inte omfattas av lämnade uppdrag bedrivas av en myndighet krävs författningsändringar eller beslut av regeringen.<sup>26</sup> Det blir normalt fallet

<sup>22</sup> Se 1 kap. 1 § tredje stycket [regeringsformen](#), 3 § [myndighetsförordningen](#) (2007:515) och 1 § andra stycket och 5 § första stycket FL förvaltningslagen (2017:900; FL). 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). Innefattar överlämnade uppgifter myndighetsutövning måste överlämnandet dessutom ha stöd i lag (12 kap. 4 § [regeringsformen](#)).

<sup>23</sup> Jfr Måste myndigheter följa lagarna? Om utkontraktering och legalitet i digital miljö, JT 2020-21 nr 2 s. 406.

<sup>24</sup> Varje enskild åtgärd som en myndighet vidtar måste inte ha uttryckligt stöd i en viss lagbestämmelse eller i andra föreskrifter som har meddelats i enlighet med 8 kap. [regeringsformen](#) – det ställs inte krav på att varje enskild åtgärd som en myndighet vidtar kan kopplas till ett specifikt bemyndigande ([prop. 2016/17:180](#) s. 59 och 289). Se även [Juridisk vägledning för verksamhetsutveckling](#) inom e-förvaltning 3.0, s. 60 och [Digitalisera rätt](#) – en praktisk juridisk vägledning, avsnitt 2.2.

<sup>25</sup> I [prop. 2016/17:180](#) har regeringen anfört bl.a. att en praxisgenomgång gett en klar indikation på att myndigheterna inte alltid i tillräcklig utsträckning tar reda på om att de har stöd i rättsordningen för sina åtgärder och att 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 också inneburit ökade risker i detta avseende (s. 58).

<sup>26</sup> 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.



när lagringsytor ska tillhandahållas av en myndighet. Här handlar det inte om verksamhet som underlättar den tjänstlevererade myndighetens kontakter med andra i samband med den egna ärendehandläggningen. Det är istället fråga om tjänster som liknar outsourcing av it-drift till privaträttsliga aktörer och tillhandahållande av anknytande infrastruktur. Tjänstlevererande myndighet kan också ha i uppdrag att utveckla och förvalta en annan myndighets tjänster eller tillhandahålla support beträffande dessa tjänster.<sup>27</sup> Här behövs normalt särskild tillåtande reglering för att kravet på legalitet ska vara uppfyllt.<sup>28</sup> Frågan om vilken rättslig styrform som bör införas över tid för myndigheter som ska tillhandahålla exempelvis nationella tekniska funktioner har närmare övervägts i Myndigheten för digital förvaltnings slutrapport Säkert och effektivt elektroniskt informationsutbyte inom den offentliga sektorn (dnr 2019-100).

## 2.9 Rättslig grund för personuppgiftsbehandlingen

Myndigheter som samverkar kring en lagringsyta måste var för sig tydliggöra den rättsliga grunden enligt dataskyddsförordningen för den personuppgiftsbehandling som kommer att utföras i varje lagringsyta och informationsutbyte.

Närbesläktad med legalitetsprincipen, är frågan om rättslig grund för personuppgiftsbehandlingen. Den europeiska dataskyddsregleringen utgår från att varje behandling av personuppgifter måste vila på en rättslig grund. I dataskyddsförordningen räknas dessa rättsliga grunder upp i artikel 6.1.<sup>29</sup>

För myndigheter och andra inom offentlig verksamhet är vanligen följande grunder tillämpliga: rättslig förpliktelse, uppgift av allmänt intresse eller myndighetsutövning samt avtal. Myndigheter får inte använda sig av en intresseavvägning när de fullgör sina uppgifter.

Det är viktigt att samverkande myndigheter var för sig tydliggör den egna myndighetens rättsliga grund för den personuppgiftsbehandling som kommer att utföras i varje lagringsyta och informationsutbyte och att den rättsliga grunden dokumenteras.

---

<sup>27</sup> Vi har emellertid erfaren 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 alljämt anses gälla för hanteringen.

<sup>28</sup> Jfr däremot vad som sagts ovan om serviceverksamhet genom egna utrymmen eller fråga- och svarstjänster för att underlätta kontakter med och uppgiftslämnande till berörd myndighet.

<sup>29</sup> Se prop. 2017/18:105 *Ny dataskyddslag*, sid. 48ff.



Ibland finns den rättsliga grunden i en registerförfattning som gäller för myndigheten.

I andra fall kan det behövas en något bredare analys. En lämplig utgångspunkt vid bestämmandet av den rättsliga grunden enligt dataskyddsförordningen är resultatet av den undersökning som enligt legalitetsprincipen måste göras för att utröna om arbetet med lagringsytan överhuvudtaget faller inom ramen för myndighetens uppdrag (se avsnitt 2.8 Legalitetsprincipen).

## 2.10 Dataskydd

Den som tillhandahåller en lagringsyta kan vara personuppgiftsansvarig för behandlingen av personuppgifter som sker i lagringsytan, gemensamt ansvarig med den myndighet som anskaffat tjänsten eller personuppgiftsbiträde åt utkontrakterande myndighet. Utgångspunkten i denna vägledning är emellertid sådan utkontraktering av it-drift där den som anlitar tjänsteleverantören ensam blir personuppgiftsansvarig precis som om myndigheten hade skött driften i egen regi. Oavsett om det är fråga om ett gemensamt personuppgiftsansvar eller ett biträdesförhållande så ska ansvaret för behandlingen regleras skriftligen i en överenskommelse eller ett personuppgiftsbiträdesavtal. Det kan vara nödvändigt att genomföra en konsekvensbedömning avseende dataskydd.

Ref. 000001

En viktig utgångspunkt för upprätthållandet av dataskyddsregelverket är att det är klarlagt vem som är ansvarig för en behandling av personuppgifter (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.<sup>30</sup> Medlemsstaterna kan fastställa i nationell rätt vem som är personuppgiftsansvarig.

I Sverige regleras myndigheters personuppgiftsansvar ofta i en s.k. registerförfattning. Om tillhandahållandet av lagringsytan regleras av författning så kan även personuppgiftsansvaret framgå av författningsregleringen. Om det inte finns någon bestämmelse om vem som är personuppgiftsansvarig för personuppgiftsbehandlingen som äger rum i lagringsytan så avgörs personuppgiftsansvaret av vem som bestämmer ändamål och medel med behandlingen. Själva grunden för personuppgiftsbehandlingen kan vara relevant att ta i beaktande vid bedömningen av vem som är personuppgiftsansvarig, innebärande att när grunden för personuppgiftsbehandlingen är att utföra en uppgift av

<sup>30</sup> 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?'"





allmänt intresse – som kommer till uttryck genom exempelvis ett regeringsbeslut – så kan ansvaret härledas från den uppgift som ålagts myndigheten.<sup>31</sup> En utgångspunkt för bedömningen av personuppgiftsansvar är att det är den som utkontrakterat och använder it-tjänsten – och inte tillhandahållaren av tjänsten – som är personuppgiftsansvarig för den personuppgiftsbehandling som användaren utför i lagringsytan. Personuppgiftsansvaret åvilar därför normalt den utkontrakterande myndigheten, dvs. användaren, medan tillhandahållaren agerar som personbiträdare. Den personuppgiftsansvarige ska teckna ett personuppgiftsbiträdesavtal med tillhandahållaren av lagringsytan.

Det kan emellertid också vara så att den myndighet som tillhandahåller lagringsytor omfattas av en registerförfattning. Den tjänstelevererande myndigheten behöver då första ställning till om registerförfattningens tillämpningsområde innefattar de nu aktuella behandlingarna. Ofta är det inte så. När så är fallet anges vanligtvis i registerförfattningen vilket organ som ska bära personuppgiftsansvaret, se domstolsdatalagen (2015:728) där det föreskrivs att varje domstol ensam är ansvarig för den personuppgiftsbehandling som den domstolen utför, trots att it-driften sköts av Domstolsverket. Enligt regeringen skulle ett delat eller gemensamt personuppgiftsansvar (mellan en domstol och Domstolsverket) medföra beaktansvärda nackdelar, inte minst gränsdragningsproblem och otydligheter (prop. 2014/15:148 s. 34).

Det kan även tänkas att personuppgiftsansvaret är delat eller gemensamt mellan tillhandahållaren och användaren. Om det är fråga om ett gemensamt personuppgiftsansvar så ska de ansvarigas respektive ansvar för att uppfylla skyldigheterna enligt dataskyddsförordningen fastställas i ett inbördes arrangemang, lämpligen genom en skriftlig överenskommelse. Är det fråga om ett biträdesförhållande ska den personuppgiftsansvarige användaren av lagringsytan teckna ett personuppgiftsbiträdesavtal med tillhandahållaren av den.

Innan en lagringsyta inrättas kan det krävas att den som är personuppgiftsansvarig för behandlingen av personuppgifter i lagringsytan genomför en konsekvensbedömning avseende dataskydd.

---

<sup>31</sup> Jfr Artikel 29-gruppens vägledning Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169).





## 2.11 Upphandlingsfrågor

Mellan myndigheter som är en del av samma juridiska person krävs inte upphandling. Tillhandahålls lagringsytor utan ersättning krävs inte upphandling.

Även om en lagringsyta tillhandahålls mot ersättning behöver den myndighet som anskaffar lagringsytan inte tillämpa det upphandlingsrättsliga regelverket<sup>32</sup> om den myndighet som tillhandahåller lagringsytan (tjänstelevererande myndighet) och den som anskaffar lagringsytan är statliga myndigheter och därmed ingår i samma juridiska person. I så fall blir det fråga om en transaktion inom den juridiska personen staten och inte något kontrakt i upphandlingsrättslig mening, vilket är avgörande för om upphandlingsplikt föreligger eller inte. Denna bedömning grundas på Konkurrensverkets ställningstagande 2018:1 (Dnr 514/2018).<sup>33</sup>

Om den myndighet som anskaffar lagringsytan däremot är en icke-statlig myndighet, exempelvis en kommun, medan tjänstelevererande myndighet är en statlig myndighet, blir det upphandlingsrättsliga regelverket tillämpligt på samma sätt som om den tjänstelevererade myndigheten vore en privat leverantör.

Behöver den myndighet som anskaffar lagringsytan inte betala någon ersättning för tjänsten är det emellertid normalt fråga om en benefik transaktion som inte behöver konkurrensutsättas enligt upphandlingsregelverket. Man ska här komma ihåg att det är den anskaffande myndigheten som vid en eventuell överprövning ska kunna visa att det rör sig om en benefik transaktion och inte ett upphandlingspliktigt kontrakt. Vid en överprövning ska domstolen nämligen göra en bedömning av samtliga omständigheter kring transaktionen för att avgöra dess egentliga karaktär. Om det då visserligen har avtalats om ett tillhandahållande utan ersättning i pengar, men man har kommit överens om annan kompensation med ekonomiskt värde, påverkar detta naturligtvis bedömningen. Detta gäller generellt för all anskaffning och bör hållas i minnet även vid anskaffning av så kallad freeware. Om myndigheten skaffar till exempel en programvara utan att det finns krav på motprestation, men den anskaffningen innebär att myndigheten sedan är bunden till en miljö som framgent kräver köp av kompletterande produkter och tjänster, kan det påverka bedömningen av när ett upphandlingspliktigt kontrakt har uppkommit.

<sup>32</sup> De svenska upphandlingslagarna utgörs av lagen (2016:1145) om offentlig upphandling ("LOU"); lagen (2016:1146) om upphandling inom försörjningssektorerna ("LUF"); lagen (2016:1147) om upphandling av koncessioner ("LUK") och lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet ("LUFS").

<sup>33</sup> Upphandlingsmyndigheten noterar dock på sin webbplats att rättsläget är oklart.



## 3. Praktisk utformning och användning

### 3.1 Att tillhandahålla lagringsytor och infrastruktur

Flera myndigheter har som framgått i uppdrag att utveckla och tillhandahålla funktioner för att förenkla uppgiftshandlingen för andra myndigheter eller för företag och privatpersoner. Det är inom detta område som lagringsytor och tillhörande infrastruktur etableras. Dessa funktioner behöver utformas så att de juridiska gränserna mellan myndigheter och mellan myndigheter och enskilda kan upprätthållas. Därför behöver det klargöras vilken roll var och en ska ha inom den digitala miljö som etableras och om en myndighet som tillhandahåller en lagringsyta ska använda de uppgifter som hanteras där för egen räkning eller bara lagra och bearbeta uppgifter där för annan och förse med tillhörande infrastruktur.

När det har bestämts vem som ska tillhandahålla lagringsytor och tillhörande infrastruktur och vilka som ska bruka dessa funktioner, som en del av sitt verksamhetssystem eller på annat sätt, behöver funktionerna utformas så att gränserna mellan myndigheter och mellan myndighet och enskilda inte bryts igenom. Dessa gränser kan upprätthållas med stöd av de grundfunktioner som beskrivits i avsnitt 2.4 och genom att uppfylla de krav på lagringsytor som redovisats i avsnitt 2.6. Från offentlighetssynpunkt kan detta ske, antingen så att en myndighets uppgifter inte görs tillgängliga för utomstående, se 2 kap. 6 § tryckfrihetsförordningen (TF), eller genom att tillgängliggjorda uppgifter hanteras så att de omfattas av ett undantag från allmän handling, se 2 kap. 13 § första stycket och 14 § första stycket 1 TF. Tydliga gränser behövs vidare för att det ska stå klart när handlingar i förvaltningsrättslig mening ska anses ha kommit in till eller expedierats från en myndighet.

I det följande ska exempel ges på hur lagringsytor och tillhörande infrastruktur etablerats, delvis med stöd av den rättspraxis och de uttalanden i lagmotiv som berörts i kap. 2 och närmare redovisats i eSams publikation Eget utrymme hos myndighet – en vidareutveckling. En myndighet som redan har resurser och erforderlig kompetens inom området kan ta fram ändamålsenliga funktioner som andra myndigheter sedan kan använda som om de hade utvecklat dem själv. Därmed behöver inte varje myndighet etablera tekniska funktioner som är av samma eller liknande slag för att fylla i huvudsak samma syften.

Utvecklingen av lagringsytor och tillhörande infrastrukturer sker i snabb takt. Vanligtvis fungerar en myndighet som ledningsaktör, även kallad byggblocksansvarig, så att myndighetssamverkan över organisationsgränser kan underlättas och att nationell digital



infrastruktur såsom Svensk e-legitimation och Mina Meddelanden kan tas tillvara fullt ut. I det följande ges exempel på några områden där funktioner av beskrivet slag har etablerats. Vid denna redovisning beaktar vi inte bakomliggande utkontrakteringar.

### 3.2 Exemplet studiestartstöd

Den byggblocksansvariga myndighetens roll kan beskrivas utifrån de funktioner för kommuner som Centrala studiestödsnämnden (CSN) har infört för studiestartstöd. Prövning av ett ärende om sådant stöd sker i två steg.

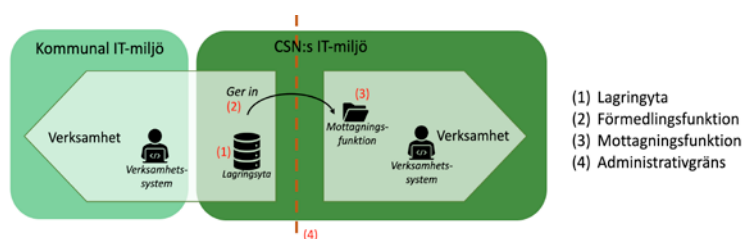
Först ansöker den enskilde om detta stöd hos sin hemkommun, normalt vid ett personligt besök hos en handläggare. Om vissa grundläggande förutsättningar är uppfyllda lämnar kommunen den enskildes ansökan med tillhörande handlingar till CSN för prövning. CSN expedierar därefter sitt beslut till sökanden. För kommunerna tillhandahåller CSN lagringsytor där de handlingar som skulle ha förekommit i en kommuns verksamhetssystem istället hanteras i CSN:s driftmiljö som ett led i en teknisk lagring för kommunens räkning. De handlingar som en kommun har på sin lagringsyta hos CSN ska därmed inte vara allmän handling hos CSN.

När kommunen är färdig med sin ärendehandläggning, som baserats på handlingarna i lagringsytan hos CSN, expedierar kommunen materialet till CSN:s mottagningsfunktion för handlingar om studiestartsstöd. Efter att handlingarna överförts till CSN:s mottagningsfunktion lagras de i CSN:s verksamhetssystem för ärenden om studiestartsstöd.

Samma handling, men i olika exemplar kan därmed finnas både i den av CSN åt kommunen tillhandahållna lagringsytan och i CSN:s verksamhetssystem efter att kommunen gett in handlingen till CSN.

Om vi utgår från de grundfunktioner som redovisats i figuren i avsnitt 2.4 tillhandahåller CSN en lagringsyta åt berörd kommun. Den ska uppfylla de krav som redovisats i avsnitt 2.6 ovan (se 1 i följande figur). CSN tillhandahåller vidare stöd för meddelandeförmedling, (se 2 i följande figur, jfr figuren i avsnitt 2.4 ovan beträffande befodringsfunktionen). CSN har dessutom inrättat en mottagningsfunktion för handlingar som ges in till CSN från en lagringsyta (se 3 i följande figur). Vid 4 i figuren anges med en streckad linje inom vilka delar respektive aktör förfogar över uppgifter.<sup>34</sup>

<sup>34</sup> Se beträffande 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? Däremot finns ingen fråga- och svarstjänst.



CSN:s hantering av kommunens uppgifter – på lagringsytan och av handlingar som mottas där eller förmedlas till mottagningsfunktionen – anses ske endast som led i teknisk bearbetning eller teknisk lagring för kommunens räkning eller endast för befordran av meddelande (2 kap. 13 och 14 §§ TF). Frågan om vilka krav som måste uppfyllas från offentlighetssynpunkt när det gäller CSN:s personals åtkomst till lagringsytor och förmedlade meddelanden har analyserats i VL eget utrymme (särskilt avsnitt 3.2.3). Vad som framkommit där ger fog för bedömningen att nödvändiga åtgärder för att rätta fel i system eller för att vidta åtgärder av informationssäkerhetsskäl kan vidtas, inom ramen för ändamålsenliga begränsningar och skydd mot olovlig åtkomst, utan att handlingar i lagringsytor blir att anse som allmänna hos den myndighet som tillhandahåller lagringsytor åt andra myndigheter.

En fråga som bör nämnas i detta sammanhang är de resonemang som tidigare förts kring den fysiska platsen för hanteringen av dessa olika samling-ar av handlingar. Tidigare har vissa hävdade att det måste finnas fysiskt åtskilda servrar inom CSN för lagringsytor hos CSN respektive för CSNs mottagningsfunktion och verksamhetssystem i övrigt. Utvecklingen av nya tekniker för informationsbehandling har emellertid fört med sig att den fysiska platsen för informationsbehandlingen delvis har mist sin betydelse. Istället har avancerade logiska avgränsningar, t.ex. i form av tillträdeskontroller, kryptering och andra liknande logiska skydd, alltmer kommit att suddas ut de fysiska gränserna. De juridiska bedömningarna kan därmed inte längre grundas på närmast fysiska frågor om lagringsplats och lagringsätt.

Eftersom respektive kommun ansvarar för de uppgifter kommunen har på sin lagringsyta gäller samma regler om bevarande och gallring som om kommunen hade hanterat uppgifterna i sitt eget verksamhetssystem.



### 3.3 Naturvårdsverket

En fortsatt beskrivning kan utgå från de funktioner som Naturvårdsverket till följd av tidigare regeringsuppdrag utvecklar för sin egen och kommunernas hantering av uppgifter i enlighet med förordningen (2018:471) om medelstora förbränningsanläggningar. För att säkerställa en tillgång till jämförbara digitala uppgifter om medelstora förbränningsanläggningar från samtliga berörda tillsynsmyndigheter<sup>35</sup> (här kommuner) etablerar Naturvårdsverket, i samverkan med kommunerna, tekniska lösningar enligt ett redovisat regeringsuppdrag.<sup>36</sup>

I praktiken innebär det att Naturvårdsverket utvecklar och tillhandahåller en nationell teknisk lösning för verksamhetsutövares underrättelser till berörd kommun om sin anläggning. Detta sker för kommunens registerhållning av anläggningsuppgifter, samt för kommunens utlämnande av uppgifter till Naturvårdsverket (för rapportering till EU).

Verksamhetsutövaren lämnar uppgifter till sin kommun via en av kommunen anvisad e-tjänst med eget utrymme för den inloggade verksamhetsutövaren. När verksamhetsutövaren, efter ifyllande och viss egen hämtning av uppgifter från andra myndigheter, väljer att skriva under och lämna in uppgifterna till sin kommun, överförs uppgifterna till kommunens mottagningsfunktion. Den mottagna handlingen ankomststämplas där och lagras på tillsynsmyndighetens lagringsyta. I samband med ankomststämplingen underrättas tillsynsmyndighetens handläggare, och ges åtkomst till den inkomna handlingar på lagringsytan via sitt ordinarie verksamhetssystem för tillsyn som har integrerats<sup>37</sup> med den nationella tekniska lösning där kommunens mottagningsfunktion och lagringsyta finns.

Den nationella tekniska lösningen innehåller<sup>38</sup> även en funktion för automatiserat utlämnande av uppgifter på begäran, från respektive kommun till en mottagningsfunktion hos Naturvårdsverket för EU-rapportering. Detta uppgiftslämnande sker automatiserat genom en sådan teknisk funktion för fråga och svar som har beskrivits i HFD 2015 ref. 61 (det s.k. LEFI Onlinemålet). Uppgifter blir tillgängliga för Naturvårdsverkets handläggare först då de nått verkets mottagningsfunktion (det vill

<sup>35</sup> I budgetpropositionen för 2020 har regeringen anförut följande: ”SKL konstaterar i Ekonomirapporten maj 2019 att förutsättningarna varierar mellan stora och små kommuner. Mindre kommuner har svårare att på egen hand effektivisera med digitalisering, däremot har de möjlighet att successivt implementera arbetssätt, system och metoder som utvecklats av andra eller tillsammans med andra.”

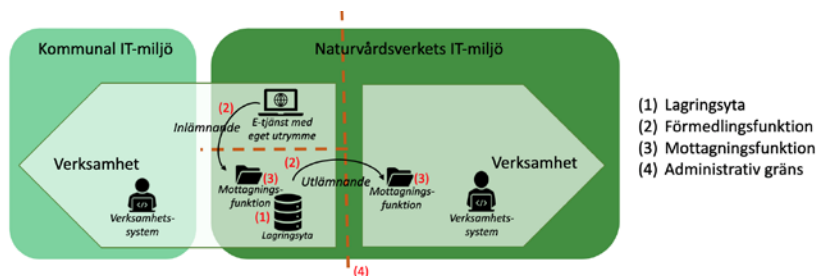
<sup>36</sup> Förslag till svenskt genomförande av direktiv 2015/2193/EU om begränsning av utsläpp till luften av vissa föroreningar från medelstora förbränningsanläggningar.

<sup>37</sup> Denna funktionalitet är inte realiserad ännu. För närvarande notifieras, och överförs uppgifter på PDF-format till, tillsynsmyndigheten m h a automatiserad e-post.

<sup>38</sup> Denna funktionalitet är inte realiserad ännu. För närvarande har Naturvårdsverket ingen åtkomst till uppgifter via den nationella tekniska lösningen.



säga inkommit till myndigheten) och överförs till handläggarens verksamhetsstöd för EU-rapportering.



Om vi utgår från de grundfunktioner som beskrivits tillhandahåller Naturvårdsverket alltså för tillsynsmyndighetens räkning en sammanhållen teknisk lösning som innehåller:

- en i juridisk mening separat (men från driftsynpunkt samordnad) e-tjänst för varje tillsynsmyndighet som ger stöd för verksamhetsutövare att ge in uppgifter till berörd kommun (2),
- en i juridisk mening separat (men från driftsynpunkt samordnad) mottagningsfunktion för varje kommun (3),
- en i juridisk mening separat (men från driftsynpunkt samordnad) lagringsyta för varje kommuns lagring av uppgifter (1),
- en i juridisk mening separat (men från driftsynpunkt samordnad) fråga- och svarsfunktion för respektive kommuns utlämnande av uppgifter till Naturvårdsverket (2)

Naturvårdsverket tillhandahåller också stöd för kommuner att ge in uppgifter till Naturvårdsverkets mottagningsfunktion för att uppgifter från kommuner till Naturvårdsverkets verksamhetsstöd för EU-rapportering.

Hantering av kommuners uppgifter på respektive lagringsyta som Naturvårdsverket tillhandahåller och den förmedling som sker till mottagningsfunktioner avses ske endast som led i teknisk bearbetning eller teknisk lagring för kommunens räkning eller endast som led i en meddelandeförmedling (2 kap. 13 och 14 §§ TF). Genom att etablera motsvarande hantering som i exemplet med studiestartstöd (se avsnitt 3.2) uppfyller Naturvårdsverket de juridiska kraven när det gäller lagringsytor, mottagningsfunktioner, meddelandeförmedling och Naturvårdsverkets personals åtkomst till uppgifter när det är nödvändigt för att rätta fel i system eller vidta åtgärder från informations-säkerhetssynpunkt.

Dessutom införs en fråga- och svarsfunktionen för varje kommun, utformad så att det inte anses uppkomma någon sådan tillgänglighet till kommuners handlingar att de blir



allmänna hos Naturvårdsverket eller hanteras i strid med reglerna om sekretess. Även här är det tillräckligt med säkra logiska avgränsningar mellan berörda aktörers uppgiftssamlingar. Eftersom respektive kommun ansvarar för de uppgifter kommunen har på sin lagringsyta gäller samma regler om bevarande och gallring som om myndigheten hade hanterat uppgifterna i sitt eget verksamhetssystem.

### 3.4 Domstolarnas verksamhetsstöd

Domstolsverket har enligt 1 § förordningen (2007:1073) med instruktion för Domstolsverket i uppgift att ge administrativt stöd och service åt domstolarna. Inom ramen för denna uppgift tillhandahålls flera verksamhetsstöd, bland annat Vera som är ett gemensamt system för domstolarna där förutom meddelade domar även utkast till avgöranden och andra handlingar hanteras. Dessa handlingar omfattas i många fall av sekretess hos domstolarna.

Vid målhanteringen är domstolarna skyldiga att använda Vera.<sup>39</sup> Dessutom är ett domstolsgemensamt e-arkiv under införande.<sup>40</sup> Det finns därmed förutsättningar att digitalisera alla akthantering och att etablera en digital infrastruktur för alla myndigheter inom Sveriges domstolar där kommunikationen kan ske digitalt även med parter och andra berörda i mål och ärenden. Domstolsverket förser också domstolarna med e-tjänster som respektive domstol avses tillhandahålla åt de som använder e-tjänsten. En fortsatt beskrivning kan utgå från de funktioner som tillhandahålls vid en elektronisk ansökan till en tingsrätt om äktenskapsskillnad.

Makarna loggar in i ett eget utrymme, upprättar sin ansökan och skickar den till domstolens mottagningsfunktion, varefter domstolen med användning av den lagringsyta verket tillhandahåller, som även innefattar domstolens verksamhetssystem, meddelar dom och expedierar den. Om vi utgår från de grundfunktioner som beskrivits tillhandahåller Domstolsverket alltså för varje domstols räkning en sammanhållen teknisk lösning som innehåller:

- en i juridisk mening separat (men från driftsynpunkt samordnad) e-tjänst för varje domstol som handlägger mål om äktenskapsskillnad,
- en i juridisk mening separat (men från driftsynpunkt samordnad) mottagningsfunktion för varje domstol (3),

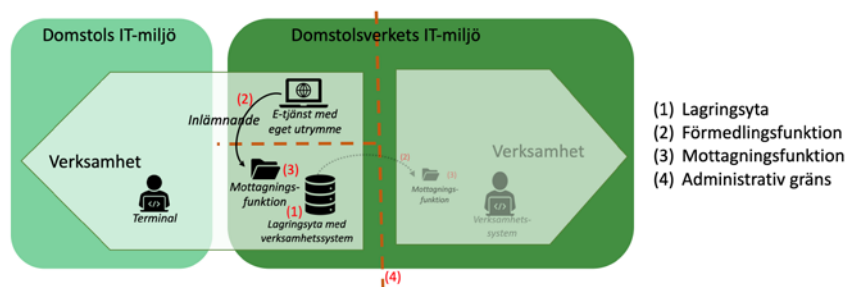
<sup>39</sup> Att domstolarna ska använda Vera för registrering av mål m.m. föreskrivs av Domstolsverket för de olika domstolsslagen, se DVFS, 2006:9 2006:11, 2006:15, 2010:3, 2011:3 och 2011:5.

<sup>40</sup> Se <https://www.regeringen.se/4ada69/contentassets/c1f239eb5b6c404ba354dd4badbd5a9d/domstolsverket-bor-ges-ratt-att-foreskriva-om-att-domstolarna-ska-anvanda-e-arkivet.pdf>.





- en i juridisk mening separat (men från driftsynpunkt samordnad) lagringsyta för varje domstols lagring av uppgifter där även domstolens verksamhetssystem finns eftersom domstolen hos sig endast brukar datorer med webbgränssnitt (1), och
- ett i juridisk mening separat (men från driftsynpunkt samordnat) e-arkiv för varje domstol, se följande figur där Domstolsverkets mottagningsfunktion och verksamhetssystem gråmarkerats eftersom de inte används i domstolens dömande verksamhet.



Exemplet kan byggas på med digitala funktioner för underrättelse om domar till andra aktörer och funktioner för att hämta uppgifter till eget utrymme m.m. Av intresse är vidare att Domstolsverket samtidigt tillhandahåller hjälptjänster, förvaltning och utveckling samt viss produktion av statistik, se avsnitt 2.4. Även Domstolsverket har en mottagningsfunktion och ett eget verksamhetssystem med hjälp av vilka domstolarna kan kommunicera med verket, men dessa funktioner har gråmarkerats i figuren eftersom de inte används i exemplet med en ansökan om äktenskapsskillnad.

Hantering i eget utrymme av utkast till ansökan sker endast som led i teknisk bearbetning och lagring för utrymmesinnehavarnas räkning och överföringen till domstolens mottagningsfunktion endast som led i en meddelandeförmedling (2 kap. 13 och 14 §§ TF). Genom att uppfylla de krav vi har beskrivit ovan uppfyller Domstolsverket de juridiska förutsättningarna när det gäller lagringsytor, mottagningsfunktioner, meddelandeförmedling och Domstolsverkets personals åtkomst till uppgifter när det är nödvändigt för att rätta fel i system eller vidta åtgärder från informations-säkerhetssynpunkt, se redovisningen ovan av kammarrätten i Jönköpings dom den 5 mars 2020 ([mål nr 3610-19](#), den s.k. VERA-domen). Detta exempel visar att fullskalig utkontraktering redan förekommer.



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 ta fram stöd och vägledningar som ger förutsättningar för att öka den digitala samverkan inom offentlig förvaltning.

Alla stöddokument finns på [esamverka.se](http://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