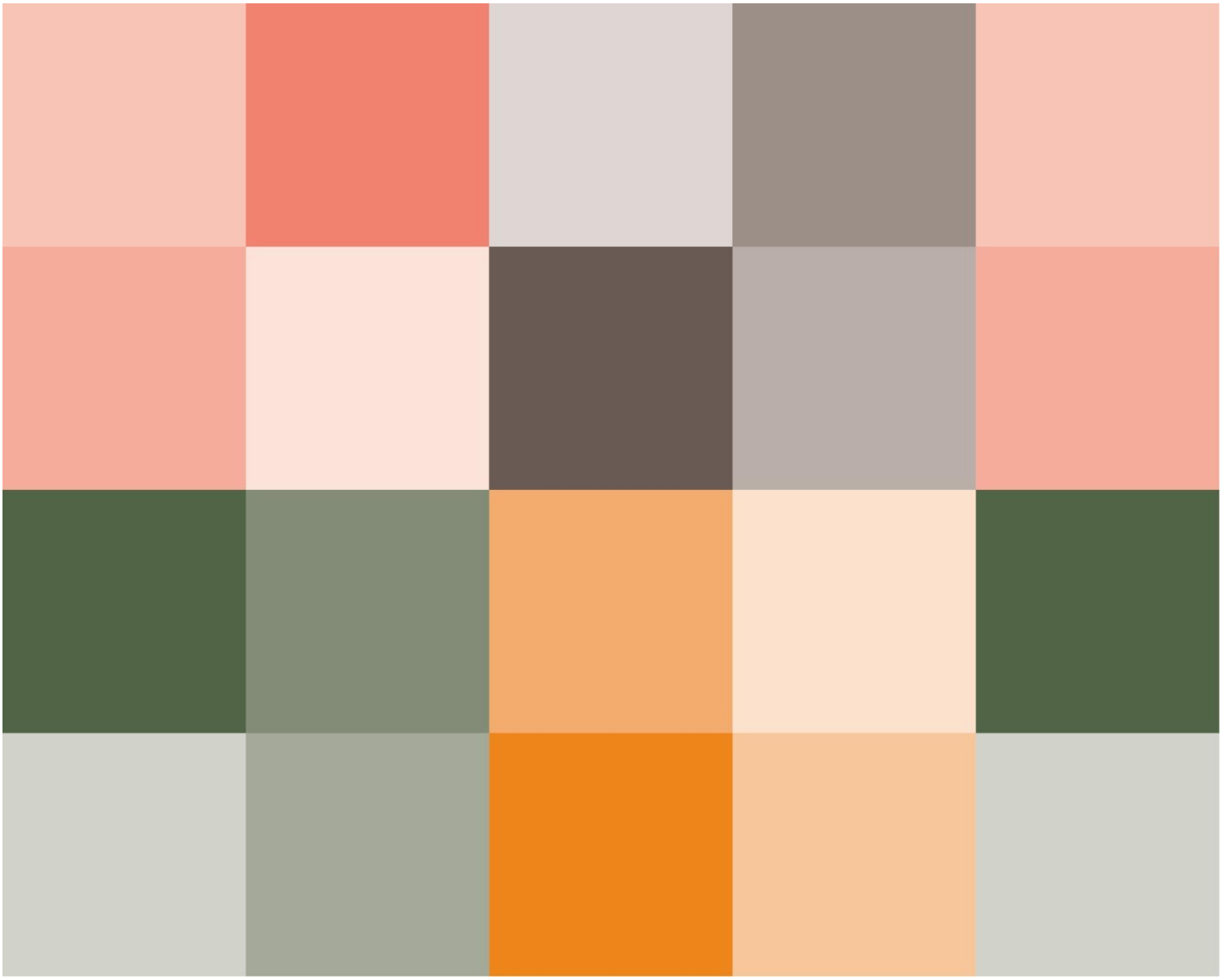


Bilaga 3

Övergripande juridisk analys av möjligheterna att öka insynen och kontrollen för individer (från Uppdrag att möjliggöra lösningar för individen till kontroll och insyn av data om individen)

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Innehållsförteckning

1 Inledning

I regeringsuppdraget Insyn och kontroll[1] ingår bland annat att föreslå en lösning för hur individer ska få en utökad insyn i vilka personuppgifter som offentliga aktörer, och i förlängningen även privata aktörer, behandlar om dem. Individer ska genom lösningen även få en utökad kontroll över sina uppgifter på så sätt att de bland annat ska kunna utöva sina rättigheter enligt EU:s dataskyddsförordning[2] digitalt och få en utökad möjlighet att överföra uppgifter mellan aktörer i olika sammanhang.

Uppdraget ska presentera en eller flera modeller som innebär att individen på ett enkelt sätt ska få information om vilka personuppgifter som olika myndigheter, och i förlängningen även privata aktörer, behandlar om individen (insyn) och en ökad möjlighet att använda de uppgifterna för olika ändamål (kontroll). En sådan användning kommer att innebära att uppgifter delas, d.v.s. lämnas ut, till tredje part. De tekniska lösningarna som kommer att utforma modellen påverkar de rättsliga frågorna som uppstår. Man kan säga att beroende på modellens tekniska lösningar, uppstår olika utmaningar utifrån ett juridiskt perspektiv. Utmaningarna grundar sig i offentlighetsprincipen, dataskyddsregleringen men även allmän förvaltningsrätt.

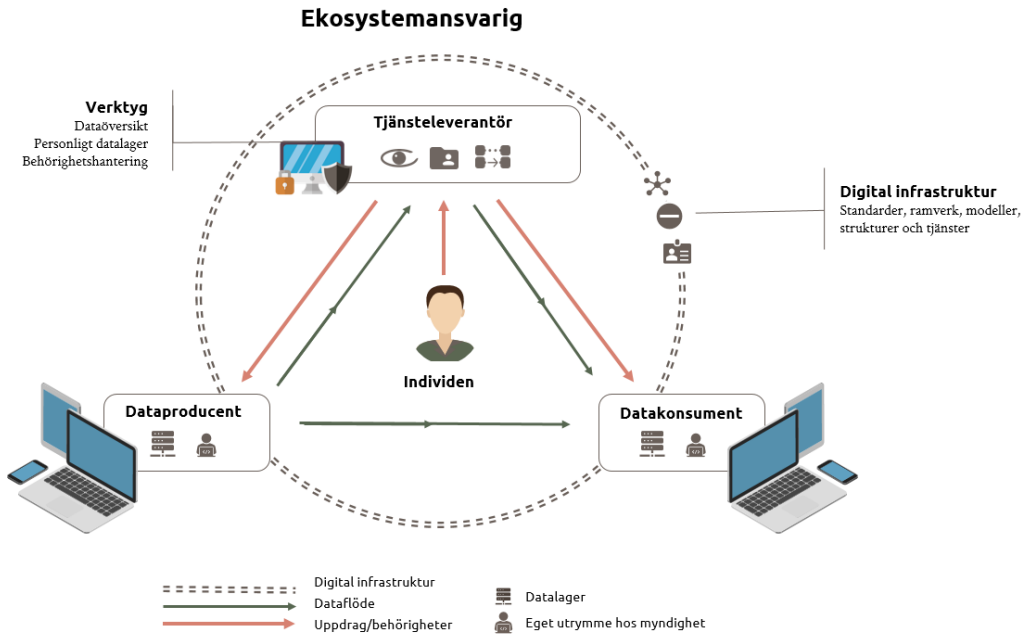
I uppdraget har en viss struktur utifrån vissa specifika roller diskuterats som en lösning för att uppnå en ökad insyn och kontroll för individen. Strukturen beskrivs i en generisk modell, vilket innebär att den beskriver händelseförlopp på ett generellt och allmängiltigt sätt. Tanken är dock att modellen ska kunna anpassas och tillämpas för specifika situationer och omständigheter. Modellen visualiseras enligt följande[3]

[1] Uppdrag att möjliggöra lösningar för individen till kontroll och insyn av data om individen (Regeringsbeslut I2020/02024/DF) sid 1-2

[2] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)

[3] För en utförligare beskrivning av modellen och vad den grundas på, se avsnitt 6 i rapporten.

Figur 1 Den konceptuella modellen av det individcentrerade dataekosystemet



Två livshändelser har diskuterats i uppdraget utifrån möjligheten att öka individens insyn och kontroll. Den ena är livshändelsen *gå till arbete* och den andra *bli sjukskriven*. Den här analysen omfattar inte en analys av de rättsliga utmaningarna som uppstår i förhållande till livshändelserna[4]. I den här analysen diskuteras endast de övergripande rättsliga frågorna som uppkommit i diskussionerna kring den generiska modellen. Nedan följer således en beskrivning av de rättsliga frågor som aktualiserats på en generell nivå. Närmare och konkreta rättsliga bedömningar kan göras först när modellen konkretiserats. Beskrivningen utgår från gällande rätt. Eftersom de rättsliga frågorna till stor del är beroende av varandra är beskrivningarna inte renodlade utifrån sakfrågan.

[4] För en juridisk analys av livshändelsen *gå till arbete*, se avsnitt 5.4 i rapporten.

2 Offentlighetsprincipen

Offentlighetsprincipen är aktuell att tillämpa för myndigheter och vissa organ[5]. Detta avsnitt är således endast relevant utifrån myndigheters perspektiv. Sammanfattningsvis är det uppdragets inställning att utlämnande av uppgifter inom modellen ska ske till individen själv efter begäran.

2.1 Generella utgångspunkter

Offentlighetsprincipen definieras i 2 kap. tryckfrihetsförordningen[6] (TF) och innebär en rätt för var och en att ta del av allmänna handlingar[7]. Rätten att ta del av allmänna handlingar får bara begränsas med hänsyn till vissa specificerade intressen och begränsningarna ska framgå av en särskild lag[8]. Den lagen är offentlighets- och sekretesslagen[9] (OSL).

I 2 kap. TF definieras bland annat vad som är en handling i TF:s mening och när en sådan är allmän[10]. En handling är en framställning i skrift eller bild eller en upptagning som endast med tekniska medel kan uppfattas på något sätt. En handling är allmän om den förvaras hos en myndighet och är inkommen dit eller upprättad där.

En uppgift i en databas kan anses vara en handling. Frågan om det är en allmän handling får göras mot bakgrund av om den är förvarad och inkommen till eller upprättad hos myndigheten.[11]

Förutom rätten att ta del av allmänna handlingar har enskilda en rätt att ta del av uppgifter ur sådana handlingar. Enligt 6 kap. 4 § OSL ska en myndighet lämna ut uppgifter ur allmänna handlingar till enskilda om de inte omfattas av sekretess och det inte stör arbetets behöriga gång.

---

[5] Jfr 2 kap. OSL
[6] tryckfrihetsförordningen (1949:105)
[7] 2 kap. 1 § TF
[8] 2 kap. 2 § TF
[9] offentlighets- och sekretesslagen (2009:400)
[10] 2 kap. 3 och 4 §§ TF
[11] En databas är inte i sig en handling då innehållet i en databas hela tiden förändras. En databas är förvisso förvarad hos en myndighet, men den omständigheten att den inte kan anses färdigställd vid någon given tidpunkt innebär att den inte kan anses vara upprättad i TF:s mening. Handlingar och uppgifter i en databas kan däremot uppfylla förutsättningarna förvarade och inkomna till eller upprättade hos myndigheten och därmed utgöra allmänna handlingar.

Det blir allt vanligare att myndigheter tillhandahåller tekniska lösningar för en annan myndighets räkning. Om någon vidtar en åtgärd endast som ett led i en teknisk bearbetning eller teknisk lagring av en handling som myndighet har tillhandahållit ska det inte anses leda till att handlingen har kommit in till den myndigheten[12]. Handlingar som förvaras endast för detta syfte är således inte allmänna hos den tillhandahållande myndigheten[13].

Offentlighetsprincipen enligt 2 kap. TF gäller endast i förhållande till enskilda. Myndigheters rätt att ta del av uppgifter framgår av 6 kap. 5 § OSL. Regleringen i 6 kap. 5 § OSL omfattar även uppgifter som inte finns i handlingar som är allmänna. Myndigheters rätt att få ut uppgifter enligt OSL är således vidare än enskildas rätt som alltså är begränsad till uppgifter ur *allmänna* handlingar.

Både offentlighetsprincipen och bestämmelserna i 6 kap. 4 och 5 §§ OSL kräver att utlämnandet sker efter begäran. Ett utlämnande från en myndighet på eget initiativ kan inte motiveras med hänvisning till nämnd reglering[14].

Dela information och frågan om allmänna handlingar

Tanken med modellen är att individen med hjälp av den ska kunna se vilka uppgifter som olika myndigheter (och i förlängningen privata aktörer) behandlar om hen (insyn), men också ha en möjlighet att dela uppgifterna med en tredje part (kontroll). De fortsatta redogörelserna utgår från att individen har identifierat sig på ett tillfredsställande sätt.

2.1.1 Utlämnande till individen själv

I en modell som syftar till att tillgängliggöra information för olika ändamål (visa och dela, ge insyn och kontroll) blir det tal om att aktörer delar information och därmed lämnar ut uppgifter. I det här sammanhanget diskuteras utlämnande av uppgifter eller handlingar till individen själv. Det kan ske efter en begäran av individen om att få ut handlingar eller uppgifter. Det kan också ske på myndighetens egna initiativ.

Utlämnande av handlingar kan ske efter begäran av individen enligt TF. Ett utlämnande av uppgifter ur allmänna handlingar kan med stöd av 6 kap. 4 § OSL.

---

[12] 2 kap. 9 § tredje stycket TF

[13] 2 kap. 13 § TF

[14] Se vidare om frågan om rättslig grund vid behandling av personuppgifter under avsnitt 4.

Utgångspunkten i den regleringen är att myndigheter ska lämna ut handlingar och uppgifter ur handlingar som i första hand är allmänna[15] och först efter en begäran.

Utlämnande av uppgifter kan ske genom att myndigheten visar information (insyn) eller lämnar ut information med möjlighet för individen att använda uppgifterna för olika syften (kontroll). Utlämnandet kan se till ett utrymme som tillhandahålls av myndigheten men som disponeras av individen på ett sådant sätt att myndigheten inte har tillgång till uppgifterna däri, ett så kallat eget utrymme[16]. Ett utlämnande till ett eget utrymme innebär att handlingar expedieras och således upprättas om detta inte skett redan tidigare[17]. Ett utlämnande som sker på begäran av den enskilda och till ett eget utrymme får anses förenligt med sekretessregleringen så länge sekretess inte gäller för uppgifterna i förhållande till den enskilda själv[18].

Det har i diskussionerna förekommit förslag på att individen ska kunna göra information tillgänglig för annan part alternativ ge i uppdrag att den skickas till annan part direkt från en myndighet (och i förlängningen privat aktör). Att begära ut uppgifter och samtidigt uppdra att de skickas till någon annan motsvarar ur ett rättsligt perspektiv att individen begär ut uppgiften själv. Utlämnandet sker alltså fortfarande på begäran av den enskilda och till den enskilda själv, även om handlingarna eller uppgifterna skickas till annan. Eftersom utlämnandet får anses ske till individen själv uppstår normalt sett inte någon sekretessproblematik. Det rekommenderas således att de tekniska lösningarna i modellen innebär att det är individen själv som vidtar en viss åtgärd som kan anses motsvara en begäran innan uppgifterna visas eller överförs.

Att begära ut uppgifter till sig själv, exempelvis till ett eget utrymme, och sedan dela uppgifterna därifrån med tredje part kallas generellt egen hämtning respektive egen delning. Eftersom det även i den här situationen blir tal om att den enskilda begär ut uppgifterna till sig själv, om än i ett första steg, för att sedan dela uppgifterna med annan part, blir det samma konsekvenser som ovan utifrån

---

[15] Jfr 2 kap. 1 § TF

[16] Se vidare om eget utrymme i avsnitt 4.

[17] Jfr 2 kap. 10 § TF. I sammanhanget ska observeras att individen enligt 6 kap. 4 § OSL har rätt att få ut uppgift ur allmän handling vid vissa förutsättningar. I den konkreta situationen måste myndigheten alltså ta ställning till om begäran avser allmän handling eller uppgift ur allmän handling. Dessutom har individen rättigheter som part i ärenden vilken inbegriper en rätt att ta del av det underlag som tillförts det aktuella ärendet. Situationen som beskrivs i texten utgår från att det rör sig om en begäran enligt TF.

[18] Jfr 12 kap. 1 § OSL; se vidare under avsnitt 2.3 om Sekretess

offentlighetsprincipen och sekretessregleringen. Bedömningen av huruvida handlingar eller uppgifter kan lämnas ut utgår från att det är den enskilda som begär till sig själv.

Det ska noteras redan i detta sammanhang att ett elektroniskt utlämnande är möjligt endast när det är tillåtet enligt den allmänna respektive särskilda dataskyddsregleringen och kan ske på ett säkert sätt[19]. Möjligheterna att dela information från ett eget utrymme med andra parter (kontroll) kan ske först när det är säkerställ att detta får ske utifrån ett dataskyddsperspektiv[20].

2.1.2 Utlämnande till annan myndighet eller enskild

2.1.2.1 Utlämnande efter begäran

Som framgår ovan kan modellen konstrueras så att funktionen att visa och dela information görs i förhållande till individen själv. En annan lösning är att information delas mellan myndighet och annan myndighet eller enskild direkt. Detta blir situationen om det är den tredje parten (annan myndighet eller enskild) som får anses begära ut handlingar eller uppgifter. Utgångspunkten i detta sammanhang är alltså att ett utlämnande initieras med anledning av en begäran från en tredje part och att utlämnandet sker direkt till den parten när förutsättningarna för ett utlämnande är uppfyllda. Utlämnande i den här situationen är inte beroende av ett eget utrymme som tillhör individen.

I det sammanhanget bör särskild hänsyn tas till det som nämns ovan om vilka handlingar respektive uppgifter som kan lämnas ut till individen själv. I förhållande till tredje part som är enskild är det endast handlingar som redan är allmänna som kan lämnas ut[21]. Detsamma gäller en begäran om att få ut uppgifter enligt 6 kap. 4 § OSL eftersom den bestämmelsen i första hand förutsätter att uppgifterna framgår av allmän handling. Om uppgifterna framgår av en handling som är allmän får utlämnande ske så länge uppgifterna inte är sekretessbelagda och det inte stör arbetets behöriga gång.

Om utlämnandet sker efter en begäran från tredje part som är myndighet sker detta enligt 6 kap. 5 § OSL. Enligt den bestämmelsen behöver begärda uppgifter

[19] Ett elektroniskt utlämnande kan bara ske i det fall det inte finns begränsningar för detta i aktuella registerlagar och utlämnandet uppfyller de grundläggande principerna i artikel 5 och säkerhetskraven enligt artikel 32 EU:s dataskyddsförordning.

[20] Se vidare under avsnitt 3

[21] Jfr 2 kap. 1 § TF

inte framgå av handlingar som är allmänna för att kunna lämnas ut. Det som kan hindra ett utlämnande i detta fall är att uppgifterna är sekretessbelagda eller att utlämnandet skulle hindra arbetets behöriga gång.

2.1.2.2 Utlämnande på eget initiativ

Modellen skulle kunna innebära att information delas generellt och direkt med samtliga aktörer, offentliga och privata, som är anslutna till modellen. Med andra ord skulle samtliga aktörer då tillgängliggöra ”sin” information för de andra aktörerna. Den här situationen har egentligen inte aktualiserats i uppdraget. Syftet med en redogörelse av ett sådant scenario är att visa på de stora rättsliga utmaningarna som skulle uppstå i det fall man skulle vilja arbeta mot en sådan lösning.

Utifrån offentlighetsprincipen har ett utlämnade av uppgifter skett (expediering) och handlingen blir då upprättad hos den tillgängliggörande myndigheten, om detta inte skett redan tidigare[22]. Den blir samtidigt inkommen till de andra myndigheterna och förvaras hos dem med den följden att uppgifterna blir allmänna handlingar även hos dem[23]. Utlämnandet får i den här situationen anses ske på respektive myndighets egna initiativ, d.v.s. utan en föregående begäran av någon part.

Det har ingen betydelse för frågan om upprättad handling om de andra aktörerna faktiskt tar del av informationen. Om informationen görs tillgänglig så att de har möjlighet att ta del av informationen är den att anse som expedierad och därmed upprättad (om detta inte skett tidigare). Detsamma gäller för frågan om handlingar är inkomna. Den omständigheten att informationen har gjorts tillgänglig för en myndighet innebär att den anses förvarad och inkommen till myndigheten[24]. Det får till följd att en teknisk lösning som innebär att information delas mellan alla myndigheter (och enskilda) som är anslutna, skapar ”nya” allmänna handlingar hos samtliga anslutna myndigheter.

Enligt 2 kap. 9 § tredje stycket TF är en handling inte att anses inkommen till en myndighet i det fall någon vidtar en åtgärd endast som ett led i teknisk bearbetning eller teknisk lagring av handlingen som en annan myndighet tillhandahållit. Handlingarna som alltså förvaras hos den tillhandahållande

[22] Jfr 2 kap. 4, 6 och 10 §§ TF.
[23] Jfr 2 kap. 6 och 9 §§ TF.
[24] Jfr 2 kap. 4, 6 och 9 §§ TF.

myndigheten är enligt 2 kap. 13 § TF inte allmänna. Detta bedöms dock inte vara situationen när information delas generellt i modellen mellan de anslutna myndigheterna på det sätt som beskrivs ovan. I en sådan situation kan inte någon myndighet anses vidta åtgärder endast som ett led i teknisk bearbetning eller lagring för någon annans räkning. I det fall regeringen uppdrar åt en myndighet att tillhandahålla och stå för driften av modellen för andra myndigheters räkning kan det bli tal om en situation där uppgifterna inte anses vara inkomna till den myndigheten som tillhandahåller lösningen. Det förutsätter dock att den tillhandahållande myndigheten inte har tillgång till informationen på något sätt för sin egen verksamhet[25].

Ytterligare två frågor aktualiseras i fallet då anslutna myndigheter delar information generellt med samtliga andra aktörer. Den första avser sekretessen. Informationen som delas får inte innehålla uppgifter som är sekretessbelagda utan att det finns ett tillämpligt undantag från sekretess alternativt en tillämplig sekretessbrytande bestämmelse. Frågan om en tillämplig sekretessbrytande bestämmelse tas upp nedan under avsnitt 2.3 Sekretess.

Den andra frågan som aktualiseras är den om rättslig grund och ett tillåtet ändamål för behandlingen som utlämnandet innebär då detta sker på eget initiativ. Den frågan omfattar även utlämnande av offentliga uppgifter. Frågan om en rättslig grund och tillåtet ändamål vid utlämnande på detta sätt aktualiseras även för privata aktörer. Frågorna diskuteras nedan under avsnitt 4 Dataskydd.

2.1.3 Särskilt om automatisk uppdatering

I uppdraget har diskuterats möjligheten att utveckla funktioner som innebär att uppgifter uppdateras automatiskt utan individens inblandning. Detta skulle liknas vid en form av prenumeration av uppgifter eller kontinuerlig delning. I dessa fall begärs en handling eller uppgift ut före den tidpunkt då den faktiskt finns eller är upprättad. Ett utlämnande enligt TF förutsätter dock att det finns en allmän handling eller uppgift vid tillfället för begäran. Om handlingen eller uppgiften som begärs ut inte finns vid tillfället för begäran är handlingen eller uppgiften inte förvarad hos myndigheten och begäran ska avslås. En kontinuerlig automatisk uppdatering, eller prenumeration, kan således bli svår att motivera utifrån utlämnanden enligt TF.

[25] Jfr 2 kap. 9 § tredje stycket och 13 § TF; se även HFD 2018 ref 48.

En lösning till detta är att den tredje parten med jämna mellanrum begär ut handlingen eller uppgiften. Ett utlämnande kan då ske om det inte hindras av sekretess. För att undvika en sekretessproblematik rekommenderas att det istället är individen själv som begär ut handlingen eller uppgiften. Om en tredje part behöver uppdaterade uppgifter bör modellen således konstrueras utifrån en funktionalitet som notifierar den enskilde om behovet av uppdatering så att uppgiften på nytt kan begäras ut av individen för vidarebefordring till den tredje parten.

2.2 Sekretess

Att dela information innebär att uppgifter tillgängliggörs och därmed röjs för den som uppgifterna avser och/eller för tredje part. Om den delade informationen innehåller uppgifter som är sekretessbelagda i förhållande till den som utlämnandet sker till, krävs därför ett tillämpligt undantag från sekretessen eller en tillämplig sekretessbrytande bestämmelse för att den utlämnande myndigheten ska kunna röja uppgifterna.

Uppgifter som omfattas av sekretess till skydd för en enskilds personliga eller ekonomiska förhållanden[26] kan i de flesta fall lämnas ut till den enskilda själv[27]. Uppgifter kan dock också omfattas av sekretessbestämmelser som är avsedda att skydda det allmännas intresse, exempelvis i olika kontroller eller inom brottsbekämpningen[28]. Om en uppgift omfattas av sådan sekretess kan den inte utan särskild prövning lämnas ut till den som uppgiften avser. Utgångspunkten för de vidare resonemangen utgår, för enkelhetens skull, från att information som kommer att delas inte innehåller uppgifter av sådan karaktär att de omfattas av sekretess till skydd för det allmänna.

2.2.1 Modellen och sekretess

Om utgångspunkten för modellen är att information om en individ endast delas med individen själv, alternativt att information delas med annan aktör på uppdrag

[26] Exempelvis 21, 25, 27 och 35 kap. OSL. Se även 40 kap. 5 § OSL och skydd för uppgift om enskilds personliga eller ekonomiska förhållanden i verksamhet för enbart teknisk bearbetning och lagring för annans räkning.

[27] Jfr 12 kap. 1 § OSL. Inom vissa sammanhang i Skatteverkets beskattningsverksamhet kan det dock vara så att uppgift om Enskild 2 förekommer i uppgifter om Enskild 1. Det kan då bli så att eftersom uppgifterna om Enskild 1 skyddar den personen, kan uppgifterna om Enskild 2 i det sammanhanget inte lämnas ut till Enskild 2. Sekretessen inom beskattningsverksamheten är oftast absolut vilket innebär att en skadeprövning inte ska göras. Om uppgifterna om Enskild 2 avslöjar uppgifter om Enskild 1 personliga eller ekonomiska förhållanden kan de därför inte röjas för Enskild 2. Att Enskild 2 eventuellt redan skulle ha vetskap om vissa uppgifter påverkar inte detta förhållande.

[28] Jfr 17 och 18 kap. OSL.

av individen, innebär sekretessregleringen inte några hinder[29]. Med hänsyn till gällande rätt är det därför önskvärt att lösningen byggs upp på ett sätt som innebär att individen själv är mottagare av informationen som delas, både utifrån syftet att ge insyn, men också utifrån möjligheten att ge en utökad kontroll genom möjlighet att dela informationen med andra. Om det är individen själv som delar informationen med tredje part uppstår inte någon sekretessproblematik för den tillhandahållande myndighetens räkning.

Om uppgifterna istället delas med alla anslutna aktörer, myndigheter som privata, blir det istället tal om ett utlämnande från myndighet till tredje part. Detta kan bara ske om det finns ett tillämpligt undantag från sekretessen eller en tillämplig sekretessbrytande bestämmelse, exempelvis att individen häver sekretessen genom att ge ett samtycke att uppgifter delas[30]. I den beskrivna situationen, d.v.s. när alla uppgifter delas med alla, måste utlämnandet anses ske på myndigheternas eget initiativ. Sekretessbrytande bestämmelser är många gånger utformade så att de blir tillämpliga först efter att någon begär ut uppgifterna. Den här situationen, då uppgifter lämnas ut på eget initiativ, kvalificerar sig därför inte för en tillämpning av sådana sekretessbrytande bestämmelser.

2.2.2 Särskilt om samtycke enligt OSL

Som framgår ovan finns det en möjlighet för individen att häva sekretessen som avser att skydda individens intressen[31]. Detta kan bli aktuellt i det fall en tredje part begär ut uppgifter om individen och dessa är sekretessbelagda med stöd av en bestämmelse som skyddar individens intresse. I ett sådant fall är det viktigt att myndigheterna lämnar den enskilda tillräcklig information om vad en eftergift av sekretess innebär och att samtycket enligt OSL också dokumenteras på ett adekvat sätt. I situationen då den enskilda efterger sekretessen för vissa uppgifter, vid särskilda tillfällen och i förhållande till en specifik aktör (offentlig eller privat) är detta en möjlig lösning. Lämpligheten i ett generellt och upprepat utlämnande av ”alla” uppgifter till samtliga aktörer grundat på att individen hävt sekretessen genom att lämna ett samtycke enligt OSL är i allra högsta grad tveksam. I det fallet är det mycket svårt, om ens möjligt, för individen att förutse vad hävandet av sekretessen får för konsekvenser.

[29] Utgångspunkten är att det uppgifter som kommer att delas i lösningen regelmässigt inte är av den typen att de omfattas av sekretessregler som avser skydda det allmännas intresse.
[30] Jfr 10 kap. 1 § och 12 kap. 2 § OSL
[31] Jfr 12 kap. 2 § och 10 kap. 1 § OSL

Frågan om fullmakt har diskuterats i olika sammanhang när uppgifter ska lämnas ut. Fullmakt innebär att en enskild får behörighet att rättshandla för en annan persons räkning. Uppdraget anser inte att fullmakter eller användning av fullmakter aktualiseras när tredje part (privat aktör eller myndighet) begär ut uppgifter om en viss individ. I det här fallet agerar den tredje parten inte för individens räkning utan begär ut uppgifterna för egen del. Det blir således rättsligt tveksamt att skapa en ordning där individen ger fullmakt åt en tredje part i den här situationen, särskilt när den parten är en myndighet. Individens kan istället i dessa situationer snarare ge sitt samtycke enligt OSL att häva sekretessen för de sekretessbelagda uppgifterna som den tredje parten begär ut.

Det ska i detta sammanhang framhållas att det är av stor vikt att inte använda individen i modellen på ett sätt så att det felaktigt framstår som att det är individen som begär ut uppgifter, när det i själva verket är annan part som i första hand vill ta del av uppgifterna. Detta skulle innebära att ett ombudsförhållande skapas på felaktiga grunder. Detta är särskilt angeläget när det är offentliga aktörer som motsvarar den tredje parten och det i sådana fall skulle innebära att myndigheten blir ombud för individen. Frågan om en myndighet kan agera ombud för en individ är högst tveksam men är inte särskilt utredd inom ramen för uppdraget.

2.2.3 Särskilt om generalklausulen i OSL

I sammanhanget sekretessbrytande bestämmelser är det vanligt att bestämmelsen i 10 kap. 27 § OSL, den så kallade generalklausulen, nämns särskilt. Generalklausulen är endast tillämplig i förhållande till myndigheter. Denna kan således inte användas för utlämnande till enskilda (privata aktörer). Vid tillämpningen av generalklausulen ska bedömningen göras om det är uppenbart att intresset att lämna ut en uppgift väger tyngre än det intresse sekretessen är avsedd att skydda. I bedömningen ska också hänsyn tas till vilket sekretesskydd uppgiften får hos den mottagande myndigheten. Utgångspunkten är vidare att en bedömning ska göras från fall till fall. Även om ordalydelsen inte utesluter tillämpning av bestämmelsen vid regelmässiga utlämnanden framgår av förarbetsuttalanden att sådana bör regleras särskilt[32]. En lösning som innebär att modellen konstrueras så att ”alla delar alla uppgifter med alla” blir de facto regelmässiga utlämnanden från samtliga myndigheter som är uppkopplade. Det blir då även tal om utlämnande på eget initiativ. Tillämpligheten av generalklausulen är förvisso möjlig vid utlämnande på eget initiativ, d.v.s. att

[32] Se prop. 1979/80:2 del A s. 326; prop. 2012/13:163 s. 70 och 87; prop. 2017/18:105 s. 136; se även RÅ 1993 not 138 och RÅ 1994 not 504

sekretessbedömningen inte förutsätter att uppgiften lämnas efter begäran, men mot bakgrund av omfattningen och karaktären av ett generellt utlämnade som diskuteras nu, anser uppdraget inte att generalklausulen är tillämplig.

Sammanfattningsvis är det således uppdragets inställning att ett allmänt utlämnande som sker i förhållande till samtliga anslutna parter, offentliga som privata, regelmässigt på eget initiativ inte är möjligt med stöd av generalklausulen.

3 Dataskyddsregleringen

Modellen aktualiserar många frågor avseende behandlingen av personuppgifter. I utformandet av en eventuell modell ska hänsyn tas till den allmänna dataskyddsregleringen[33] och tillämpliga registerlagar. Nedan följer en redogörelse för de frågor som uppdraget uppmärksammat i arbetet. Sammanfattningsvis är det uppdragets inställning att det kvarstår obesvarade frågor utifrån ett dataskyddsperspektiv avseende den behandling som förväntas ske inom ramarna för modellen.

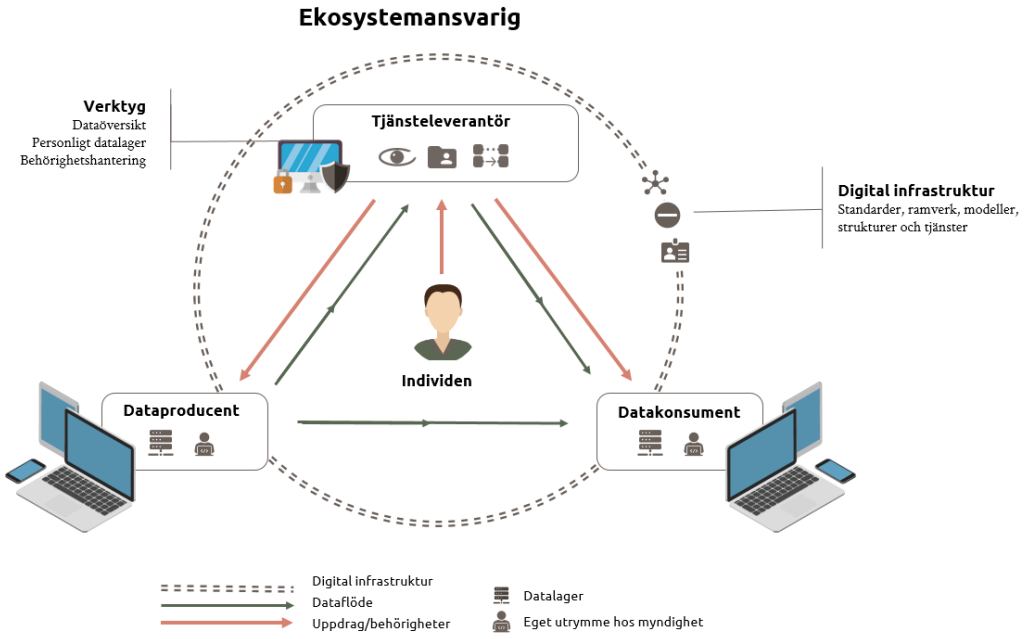
3.1 Personuppgiftsansvaret

Utifrån ett dataskyddsperspektiv definieras personuppgiftsansvarig som en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter[34]. Personuppgiftsansvaret kan regleras[35].

Om en personuppgiftsansvarig utkontrakterar sin behandling, d.v.s. låter behandlingen av uppgifterna utföras av en annan aktör för den personuppgiftsansvarigas räkning, uppstår ett personuppgiftsbiträdesförhållande. Detta ska regleras genom ett avtal eller rättsakt.[36]

Den struktur som modellen har är uppdelad i roller, där olika aktörer kan ikläda sig olika roller vid olika tillfällen. En av rollerna i strukturen är den ekosystemansvariga. Den ekosystemansvariga är den som tillhandahåller den digitala infrastrukturen med nödvändiga verktyg som möjliggör visningen av information (insyn) och delningen av information (kontroll). Modellen visualiseras genom bilden nedan[37].

[33] EU:s dataskyddsförordning, den kompletterande dataskyddslagen (2018:218) och den kompletterande dataskyddsförordningen (2018:219)
[34] Artikel 4 EU:s dataskyddsförordning
[35] Ibid.
[36] Jfr artikel 28 EU:s dataskyddsförordning.
[37] Samma bild som i inledningen.



Frågan om personuppgiftsansvaret för den ekosystemansvariga får besvaras utifrån vem som bestämmer ändamålen och medlen för behandlingen som sker där. Om rollen ekosystemansvarig tillhandahålls av olika aktörer gemensamt, offentliga eller privata eller både och, kan det bli aktuellt med ett gemensamt personuppgiftsansvar. Ett gemensamt personuppgiftsansvar ska regleras genom en överenskommelse[38]. Mot bakgrund av det stora antal aktörer som kan komma att beröras i detta sammanhang kan detta bli mycket svårt att åstadkomma[39].
Uppdraget anser därför att det är att föredra att rollen som ekosystemansvarig regleras i lag i vilken även personuppgiftsansvaret regleras och någon eller några få myndigheter pekas ut som personuppgiftsansvariga.
Att personuppgiftsansvaret är utpekat i lag hindrar inte att den eller de personuppgiftsansvariga utkontrakterar behandlingen, i det här fallet att myndigheten eller myndigheterna anlitar en privat leverantör för behandlingen. Detta förutsätter dock att möjligheten till utkontraktering finns utifrån ett

[38] Jfr artikel 26 EU:s dataskyddsförordning.
[39] I uppdraget Flytta till Sverige har berörda myndigheter bedömt att personuppgiftsansvaret är gemensamt för den tjänst som tagits fram för att underlätta för enskilda i situationen att de ska/vill flytta till Sverige. I det fallet är det dock inte så många myndigheter som berörs av tjänsten och förutsägbarhet och tydlighet både för myndigheterna själva vad gäller respektive myndighets ansvar, men också för den registrerade personen. Mot bakgrund av att modellen inte har en så begränsad användning som i fallet med tjänsten Flytta till Sverige, bör den situationen inte tjäna som förebild i det här fallet.

sekretessperspektiv och dataskyddsrättsliga principer, såsom exempelvis förbudet mot utlämnande till tredje land. I det fallet det är möjligt att utkontraktera behandlingen uppstår ett personuppgiftsbiträdesförhållande och ett personuppgiftsbiträdesavtal måste ingås i vilket tydliga instruktioner ska ges av den personuppgiftsansvariga[40].

Frågan om personuppgiftsansvaret är aktuell även i förhållande till de andra rollerna i modellen. Mot bakgrund av strukturen i modellen och rollbeskrivningen är det sannolikt att andra roller kommer att vara personuppgiftsansvariga för vissa behandlingar som aktualiseras i modellen. Detta gäller särskilt rollerna dataproducent, datakonsument och tjänsteleverantör. Det innebär att de ansvarar för att säkerställa att all den behandling de utför är tillåten och i enlighet med de grundläggande principerna i artikel 5 EU:s dataskyddsförordning. Detta inkluderar den behandling som utlämnande av uppgifter innebär.

3.2 Laglig grund

En av de grundläggande principerna för behandling av personuppgifter[41] är principen om laglighet[42]. Principen om laglighet definieras i artikel 6 EU:s dataskyddsförordning.

Om modellen innebär att myndigheter eller privata aktörer tillgängliggör uppgifter för andra myndigheter eller enskilda så blir det tal om ett utlämnande av uppgifter till myndighet eller tredje man. Utlämnande av uppgifter är en form av behandling som behöver vara rättsligt förankrad bland annat genom en laglig grund och ett tillåtet ändamål.

3.2.1 Utlämnande

3.2.1.1. Till ”alla” på eget initiativ

Om utgångspunkten är att modellen är konstruerad så att en aktör bara genom sin anslutning automatiskt lämnar ut uppgifter genom att de speglas eller lagras hos den ekosystemansvariga och därigenom tillgängliggörs för andra myndigheter eller privata aktörer, rör det sig om ett utlämnande på eget initiativ. Uppgifterna lämnas i detta fall inte ut efter en begäran av individen själv eller annan myndighet eller privat aktör. Som framgår under avsnittet om offentlighetsprincipen har detta scenario inte diskuterats som ett möjligt alternativ i uppdraget men det är

[40] Jfr artikel 28 EU:s dataskyddsförordning.
[41] Artikel 5 EU:s dataskyddsförordning
[42] Artikel 5 p. 1 a EU:s dataskyddsförordning

ändå av vikt att redogöra för de många svårigheter en sådan lösning får utifrån ett rättsligt perspektiv.

Utlämnandet i detta fall innebär en ny behandling av redan insamlade uppgifter. Ändamålet med den nya behandlingen får inte vara oförenligt med det ursprungliga ändamålet[43] med behandlingen vid insamlingen av uppgifterna. En bedömning enligt principen om ändamålsbegränsning, även kallad finalitetsprincipen, ska göras enligt förutsättningarna i artikel 6.4 EU:s dataskyddsförordning. Med tanke på att utlämnandet i detta fall sker på eget initiativ utan särskild mottagare och för okända ändamål, samt den omständigheten att uppgifterna får en stor spridning, är det uppdragets inställning att ett utlämnande på eget initiativ till samtliga anslutna aktörer generellt inte är förenligt med de ursprungliga ändamål myndigheten hade när uppgifterna samlades in. I den bedömningen har, i förhållande till myndigheters förhållanden, hänsyn tagits till att serviceskyldigheten enligt 6 § FL inte innebär en skyldighet för myndigheter att sprida information på föreslaget sätt[44]. Sammanfattningsvis är det uppdragets inställning att det, utifrån nuvarande reglering, saknas rättsliga förutsättningar för såväl myndigheter som privata aktörer, att på eget initiativ dela information med samtliga aktörer i en framtida modell.

3.2.1.2 Till tredje part efter begäran

Tredje part kan begära att få ut uppgifter om individer. Ett utlämnande kan ske med stöd av TF eller 6 kap. 4 § OSL om den tredje parten är en privat aktör. Är den tredje parten istället en annan myndighet kan ett utlämnande ske med stöd av OSL om förutsättningarna i 6 kap. 5 § den lagen är uppfyllda. Ett utlämnande enligt TF hindras inte av dataskyddsregleringen[45]. Ett utlämnande som sker med stöd av 6 kap. 4 eller 5 §§ OSL har en rättslig grund i de bestämmelserna och ändamålet med den behandling som utlämnandet innebär är i dessa fall inte oförenligt med det ursprungliga ändamålet[46]. Nuvarande dataskyddsreglering möjliggör således ett utlämnande från en myndighet till en tredje part när detta sker efter begäran.

När det gäller privata aktörer så får de göra en bedömning om huruvida det finns en laglig grund och tillåtet ändamål för den behandling som ett utlämnande från

[43] Jfr artikel 5.1 b EU:s dataskyddsförordning.
[44] Se vidare avsnitt 3.2.2.
[45] Jfr artikel 86 EU:s dataskyddsförordning samt 1 kap. 7 § kompletterande dataskyddslagen.
[46] Jfr HFD dom den 19 februari 2021, målnr 433-20

dem innebär utifrån de förutsättningar som grundar behandlingen av de uppgifter som begärs ut. Det kan dock av uppenbara skäl inte stödja sig mot regleringen i OSL.

3.2.1.3 Till individen själv

En behandling som innebär att uppgifter lämnas ut till individen själv ställer samma krav på rättslig grund och ett tillåtet ändamål. Ändamålet med behandlingen får inte vara oförenligt med det ursprungliga ändamålet som myndighet eller privat aktör hade när uppgifterna samlades in.

Ett utlämnande på eget initiativ är högst sannolikt oförenligt med det ursprungliga ändamålet med behandlingen, liksom konstaterades ovan[47]. Om ett utlämnande till individen inte sker efter en begäran är behandlingen därför sannolikt inte tillåten då den saknar en rättslig grund. För myndigheters räkning utgår detta ställningstagandet från att serviceskyldigheten enligt 6 § FL inte anses innebära en sådan skyldighet[48].

För en myndighets räkning kan ett utlämnande av en allmän handling till individen ske enligt TF när en enskild har begärt ut en handling. Uppgifter ur en allmän handling enligt 6 kap. 4 § OSL kan också lämnas ut till individen efter begäran[49]. Sammanfattningsvis har myndigheten en rättslig grund och tillåtet ändamål för sin behandling om utlämnandet av uppgifter sker efter att individen begärt ut den[50].

Enligt EU:s dataskyddsförordning har registrerade personer rätt att få ett registerutdrag efter begäran som ska visa bland annat vilka uppgifter som den personuppgiftsansviga behandlar om personen och för vilka ändamål och med vilken rättslig grund samt vem uppgifterna delas med[51]. En registrerad person har rätt att få ut ett registerutdrag kostnadsfritt en gång per år. För efterföljande begäran får en rimlig utgift tas ut. Om begäran görs i elektronisk form ska

---

[47] Utlämnande på eget initiativ är inte att likställa med utlämnande inom ramarna för ärendehantering eller annan verksamhet där förfaranderättslig eller materiell reglering kan kräva kommunicering och annat utlämnande från myndighetens sida utan en föregående begäran.

[48] Se vidare avsnitt 3.2.2.

[49] 6 kap. 4 § OSL. Det ska också i detta sammanhang framhållas kommunikation som sker inom ramarna för handläggningen av ett ärende enligt de förfaranderättsliga bestämmelser som gäller i det förfarande som aktualiseras. Detta ska skiljas från den situation som avses i texten.

[50] Observera att dataskyddslagstiftningen inte innebär ett hinder för utlämnande enligt offentlighetsprincipen, artikel 86 och 1 kap. 7 § den kompletterande dataskyddslagen.

[51] Jfr artikel 15 EU:s dataskyddsförordning

informationen tillhandahållas i ett elektroniskt format som är allmänt använt om den registrerade inte begär annat[52].

Den del av modellen som avser insyn skulle möjligtvis kunna grunda sig på rätten till ett registerutdrag. Som livshändelserna har beskrivits är det dock andra typer av uppgifter som också är tänkta att tillgängliggöras i insynsdelen och även handlingar[53]. Dessutom sträcker sig tillgången till uppgifterna såsom den är beskriven i modellen, inte lika långt enligt rätten till ett registerutdrag, som alltså endast ger rätt till ett kostnadsfritt uttag per år.

3.2.1.4 Särskilt om automatisk uppdatering

I vissa fall kan det finnas behov av att en automatisk uppdatering av uppgifter utan att individen behöver agera. Som framgår ovan är det utlämnande som uppdateringen innebär inte möjlig enligt TF eftersom att handlingen eller uppgiften som begärs ut i dessa fall inte är förvarade hos en myndighet vid tiden för begäran.

Behovet av kontinuerlig uppdatering av uppgifter kan lösas genom direktåtkomst. Utifrån ett integritetsperspektiv bör direktåtkomst dock användas restriktivt. Direktåtkomst är alltid särskilt reglerat utifrån myndigheters materiella behov och kräver stöd i registerlagstiftningen. Reglering om direktåtkomst i registerlagarna kombineras också oftast med sekretessbrytande bestämmelser. När det gäller individer är det brukligt att direktåtkomst, när den ges, avser åtkomst till de egna uppgifterna.

Uppdraget anser inte att det finns någon möjlighet att tillgodose en tredje parts tillgång till uppgifter genom direktåtkomst, och läka bristen på reglering genom att använda kontinuerlig uppdatering så som det beskrivits inledningsvis. Uppdaterad information ska inte överföras direkt till tredje part utan individens inblandning. Utlämnandet av uppgifter ska istället ske efter en tydlig begäran om uppdatering från individen som då har full insyn i vilka uppdaterade uppgifter som eventuellt kommer att delas vidare. Om uppgiften har ändrats ska individen

---

[52] Ibid.

[53] Det har i uppdraget diskuterats om rätten till ett registerutdrag enligt artikel 15 även omfattar rätten att få ut handlingar. Lydelsen i artikel 15 talar dock endast om personuppgifterna i sig och inte handlingar i vilka de ingår i. Dessa kan dessutom innehålla även andra uppgifter än personuppgifter vilka inte omfattas av rätten till ett registerutdrag. Rätten till ett registerutdrag tolkas och tillämpas inte så att även handlingar lämnas ut med stöd av artikel 15 av de deltagande myndigheterna.

uppmärksammas på detta, exempelvis genom en notis. Om tredje part behöver uppdaterade uppgifter behöver det därför finnas en funktionalitet för att notifiera individen om detta så att uppgiften på nytt kan inhämtas av individen själv för vidarebefordring.

3.2.1.5 Sammanfattande synpunkter om utlämnande

Utifrån myndigheters perspektiv är frågan om vem som begär ut uppgifter, alternativ om uppgifter lämnas ut på myndighetens egna initiativ, central att reda ut med hänsyn till vilken rättslig grund och tillåtet ändamål myndigheten har för den behandlingen som utlämnande innebär utifrån ett dataskyddsperspektiv[54]. Uppdraget har diskuterat möjligheten att luta sig mot serviceskyldigheten i 6 § förvaltningslagen (FL) i ett sådant fall. Bedömning är dock att serviceskyldigheten, såsom den kommer till uttryck idag, inte omfattar den här typen av informationsdelning[55].

Det är vår inställning, utifrån dataskyddsregleringen, att de tekniska lösningarna i modellen bör utformas så att uppgifter visas först när individen begär detta. Samma resonemang gäller för utlämnande av uppgifter till individen. Även den delen av modellen som avser kontroll, d.v.s. individens möjlighet att dela information med andra, bör tekniskt byggas upp så att detta sker först när personen aktivt väljer att göra så. Frågan om behandlingen och den rättsliga grunden för utlämnandet till tredje part på uppdrag av individen kan möjligtvis grunda sig på ett samtycke i vissa fall men bedömningen av den frågan behöver utredas vidare i samband med att detaljerna kring delningen av information och den tjänst som tas fram utvecklas.

Behov av uppdatering av uppgifter ska inte lösas genom direktåtkomst. Det ska istället lösas genom en funktionalitet som innebär att individen uppmärksammas på behovet av uppdatering och då själv kan begära ut uppgiften eller handlingen själv för att eventuellt dela den med tredje part.

---

[54] Se avsnitt 3 Dataskydd.

[55] Hjälpen till enskilda kan t.ex. bestå i att myndigheten lämnar upplysningar om hur man gör en ansökan, vilka handlingar som ska skickas med en ansökan eller hur en blankett ska fyllas i. Myndigheten kan också vägleda den enskilda genom att t.ex. anvisa hur hen bör komplettera utredningen, sträva efter begränsning av utredningen eller lämna förslag på enklare och bättre sätt för den enskilda att uppnå det som önskas. Serviceskyldigheten innebär inte att myndigheter har en skyldighet att agera åt individer eller tillhandahålla avancerade tekniska lösningar som den modell som diskuterats i uppdraget.

3.2.2 Särskilt om serviceskyldighet enligt 6 § FL som rättslig grund

Av 6 § förvaltningslagen (FL) följer att myndigheter har en serviceskyldighet i förhållande till enskilda. Serviceskyldigheten innebär att myndigheten ska lämna den enskilde sådan hjälp att han eller hon kan ta till vara sina intressen. Hjälpen ska ges i den utsträckning som är lämplig med hänsyn till frågans art, den enskildes behov av hjälp och myndighetens verksamhet. Den ska ges vid ärendehandläggning såväl som vid s.k. faktiskt handlande. Det finns inget som hindrar att en myndighet ger mer service och stöd än det som krävs enligt serviceskyldigheten enligt 6 § FL, men myndigheten måste då ta hänsyn till principen om objektivitet och likabehandling. Det ska också framhållas att FL är subsidiär i förhållande till annan särskild reglering vilket innebär att det kan finnas bestämmelser inom vissa sakområden som innebär en vidare serviceskyldighet i vissa fall.

Den hjälp som myndigheten ska ge enskilda enligt 6 § FL är begränsad till den egna verksamheten. Att på en mera generell nivå dela uppgifter med andra myndigheter och enskilda, även om det skulle vara på uppdrag av individen, ingår således inte i serviceskyldigheten såsom den kommer till uttryck idag i förvaltningslagen. Uppdraget anser inte heller att 6 § FL innebär en skyldighet för myndigheter att skicka information på eget initiativ till andra myndigheter med anledning av att uppgifterna behövs i ärendehandläggning hos den mottagande myndigheten. Den slutsatsen påverkas inte av att detta sker på uppdrag av individen. Samma resonemang gäller för eventuellt informationsutbyte mellan myndigheter och privata aktörer.

Serviceskyldigheten såsom den kommer till uttryck i 6 § FL idag kan således, enligt uppdragets inställning, inte anses utgöra den rättsliga grunden för det informationsutbyte som diskuterats i förhållande till modellen och livshändelserna.

Det är tänkbart att dagen serviceskyldighet för myndigheter enligt förvaltningslagen kan utvecklas till någonting mer omfattande. Den tekniska och digitala utvecklingen går snabbt framåt och med en sådan utveckling följer också att allmänhetens förväntningar ökar vad gäller den offentliga förvaltningens effektivitet. Det är därför rimligt att utgå från att enskilda individer förväntar sig att statliga och kommunala myndigheter följer med i den digitala utvecklingen för att säkerställa en rationell och säker informationshantering men också för att möjliggöra att den enskilde får ökad insyn och kontroll över de uppgifter som finns registrerade, om individen själv. Enskilda individer kan även ha

förväntningar att kunna återanvända myndigheters uppgifter, t.ex. för att dela uppgifterna om sig själva med en tredje part. Serviceskyldighetens innebörd kan därför behöva utvidgas till att även inbegripa en skyldighet för myndigheter att tillhandahålla en myndighetsgemensam digital infrastruktur som på ett lättöverskådligt och samlat sätt visar den enskilde de uppgifter som varje myndighet har registrerade om honom eller henne, varifrån uppgifterna härstammar, de rättigheter som den enskilde har att ändra eller radera uppgifterna och vilka möjligheter den enskilde har att återanvända uppgifterna för egna syften. Sådana tjänster för insyn och kontroll skulle möjligen kunna samlas i ett så kallat eget utrymme hos myndigheten.

En eventuell utvidgning av 6 § FL måste dock utredas vidare och konsekvenserna noggrant övervägas med anledning av bestämmelsens generella tillämplighet inom den offentliga sektorn. En utvidgning av serviceskyldigheten enligt FL som innebär en skyldighet för myndigheter att tillhandahålla och dela uppgifter, särskilt elektroniskt, kommer även att behöva kompletteras med ändringar inom den särskilda dataskyddsregleringen (registerlagar) som gäller i olika verksamheter, i vart fall vad gäller ändamålsbestämmelser men även möjligheten att lämna ut uppgifter i elektronisk form. En eventuell utvidgning av 6 § FL kommer således inte ensam att vara tillräckligt för lösa problematiken med en rättslig grund för informationsdelningen inom ramarna för modellen.

3.2.3 Särskilt om samtycke som rättslig grund

En av de lagliga grunderna är att behandlingen sker med den registrerade personens samtycke[56]. Det finns vissa villkor som ska vara uppfyllda när man behandlar personuppgifter med stöd av den registrerade personens samtycke. Den personuppgiftsansvariga ska bland annat kunna visa att den registrerade personen har samtyckt till behandlingen. Den registrerade personen ska också ha rätt att när som helst återkalla sitt samtycke.[57] Vid behandling av känsliga personuppgifter ska den registrerade ha gett ett uttryckligt samtycke till behandlingen av sådana uppgifter[58].

[56] Artikel 6 p.1 a EU:s dataskyddsförordning

[57] Artikel 7 EU:s dataskyddsförordning

[58] Skäl 43 samt artikel 9 p. 2 a EU:s dataskyddsförordning. Huvudregeln enligt artikel 9 är att känsliga personuppgifter inte får behandlas alls. Från denna huvudregel finns ett antal undantag, bland annat när behandlingen sker efter ett uttryckligt samtycke av den registrerade personen. Kravet på att samtycket ska vara uttryckligt innebär att samtycket måste vara skriftligt. Samtycket kan i detta fall inte vara underförstått genom bekräftande handlingar som den enskilda vidtar. För

Ett samtycke ska vara frivilligt och ska användas främst när maktförhållandet mellan den personuppgiftsansvariga och den registrerade personen är jämlikt.

3.2.3.1 Dataportabilitet

En av rättigheterna som registrerade personer har enligt EU:s dataskyddsförordning är rätten till dataportabilitet. Rätten till dataportabilitet innebär en rätt för den registrerade personen att få ut sina personuppgifter som han eller hon tillhandahållit den personuppgiftsansvariga i ett strukturerat, allmänt använt och maskinläsbart format och ha rätt att överföra uppgifterna till en annan personuppgiftsansvarig, när detta är tekniskt möjligt. Rätten till dataportabilitet aktualiseras dock bara när behandlingen grundar sig på ett samtycke eller ett avtal och sker automatiserat.[59] I det fall någon av behandlingarna i modellen sker med stöd av den registrerade personens samtycke aktualiseras således rätten till dataportabilitet.

3.2.3.2 Myndigheter och samtycke

De absolut vanligaste rättsliga grunderna för myndigheters behandling av personuppgifter är rättslig förpliktelse, myndighetsutövning eller ett allmänt intresse med anledning av den verksamhet som myndigheten bedriver[60].

Möjligheten för en myndighet att grunda personuppgiftsbehandling på ett samtycke är starkt begränsad, eftersom förhållandet mellan myndigheten och den registrerade personen inte är jämlikt. Dessutom kan enskilda sägas stå i en beroendeställning till det offentliga varför ett samtycke av den anledningen inte kan anses vara frivilligt på det sätt som krävs enligt EU:s dataskyddsförordning. Det kan samtidigt inte uteslutas att det finns situationer, om än få, då en myndighet kan grunda en viss behandling av personuppgifter på samtycke som laglig grund.

I de få fall, samtycke skulle kunna användas som laglig grund av en myndighet, skapas en administrativ börda för den personuppgiftsansvariga myndigheten. Förutom den dokumentation som måste finnas för att den personuppgiftsansvariga myndigheten ska kunna visa att samtycket uppfyller de krav som ställs utifrån EU:s dataskyddsförordning, finns även andra

---

mer information om vad som krävs vid samtycke se www.imy.se och Edpb:s guidline Consent under regulation 679/2016.

[59] Artikel 20 EU:s dataskyddsförordning

[60] Jfr artikel 6 p. 1 c och d EU:s dataskyddsförordning

omständigheter att beakta. Ett samtycke kan alltid återkallas och behandlingen måste då upphöra. Den registrerade personen har vidare rätt att begära dataportabilitet av sina uppgifter vilket den personuppgiftsansvariga inte får hindra.

Mot bakgrund av hur modellen presenterats och vilka övriga rättsliga ställningstaganden som gjorts i relation till denna, bland annat för att möjliggöra delning av information, är det uppdragets inställning att samtycke som laglig grund inte kan användas av myndigheter för behandling av personuppgifter i modellen som sådan. Möjligtvis kan vissa behandlingar, exempelvis ett utlämnade från ett eget utrymme, grunda sig på den registrerade personens samtycke.

3.3 Elektroniskt utlämnande

De utlämnanden som modellen aktualiserar innebär att personuppgifter lämnas ut elektroniskt. I många registerlagar är det särskilt reglerat vid vilka förutsättningar ett elektroniskt utlämnande av uppgifter får ske till enskilda[61], och ibland även till myndigheter[62]. Det måste således säkerställas att aktuella uppgifter får lämnas ut elektroniskt från olika verksamheter. Ett elektroniskt utlämnande kan ske via medium eller direktåtkomst.

Mot bakgrund av hur modellen beskrivits tekniskt är det troligtvis tal om utlämnanden på medium. Vi vill ändå framhålla att vi rekommenderar att modellen och olika lösningar i modellen inte innebär att direktåtkomst ges till någon part. Direktåtkomst innebär ett större intrång utifrån ett integritetsperspektiv och spridningen av uppgifter blir större. Vid egen hämtning respektive delning av uppgifter, d.v.s. när individen begär ut uppgifter för att sedan dela dem med annan part, bör därför funktionen utformas så att uppgifterna inhämtas först efter en uttrycklig begäran, så att endast de uppgifter som begärts ut också lämnas ut[63]. Detsamma gäller vid omedelbar hämtning, d.v.s. när tredje part begär ut uppgifterna. Funktionen bör även i dessa fall utformas så att uppgifterna lämnas ut först efter begäran till en annan myndighet eller privat

[61] Jfr exempelvis 2 kap. 6 § SdbL, 2 kap. 6 § FdbL,

[62] Jfr elektroniskt utlämnande från socialförsäkringsdatabasen där lagstiftaren ansett att även utlämnande till myndigheter har begränsats, förordning (2003:766) om behandling av personuppgifter inom socialförsäkringens administration; se även SOU 2015:39 s. 432.

[63] Jfr principen om uppgiftsminimering, artikel 5 1. C EU:s dataskyddsförordning

aktör och utlämnandet endast ske av de uppgifter som begärts ut. Vi behöver också säkerställa att utlämnandet kan ske på ett säkert sätt.[64]

3.4 Frågan om säker behandling

Frågan om säkerhet vid behandlingen[65] är en grundläggande princip och central för all behandling. Modellen kräver en säkerhetsnivå som är anpassad till de kategorier av uppgifter som kommer att behandlas. Kravet på spårbarhet, behörighetssättning m.m. måste beaktas vid samtliga behandlingar inom modellen. Modellen bygger på att insyn och kontroll ska kunna ske helt digitaliserat. Detta kräver en infrastruktur som är tillräckligt säker utifrån de krav som ställs upp i EU:s dataskyddsförordning. I dagsläget finns inte en sådan infrastruktur för en generisk modell som ska tillämpas myndighetsgemensamt och som möjliggör även en möjlighet för privata aktörer att ansluta sig till. Det finns dock vissa initiativ som är sektorspecifika där myndigheter samarbetar för att tillhandahålla information och tjänster utifrån en viss händelse[66].

Det arbete som uppdraget en förvaltningsgemensam digital infrastruktur för informationsutbyte kan vara relevant att följa utifrån detta perspektiv. En sådan struktur skulle möjligtvis kunna tjäna som en säker infrastruktur för modellen och möjligtvis motsvara rollen ekosystemansvarig, i vart fall när aktörerna är uteslutande offentliga[67].

3.5 Övriga grundläggande principer

Förutom de grundläggande principerna som redan lyfts ska personuppgiftsansvarig säkerställa att de övriga grundläggande principerna[68] uppfylls. I detta sammanhang blir frågan om uppgiftsminimering respektive lagringsminimering viktig att ta ställning till. I situationen där uppgifter delas av alla med alla, så att säga, på eget initiativ uppfyller den personuppgiftsansvariga inte principen om uppgiftsminimering. Det är endast de uppgifter som krävs för ändamålet som ska behandlas vilket inte är situationen vid en lösning som innebär allmän delning.

---

[64] Jfr artikel 32 EU:s dataskyddsförordning när det gäller personuppgifter

[65] Jfr artikel 5 1. f och artikel 32 EU:s dataskyddsförordning

[66] Exempel på sådana initiativ är Flytta till Sverige, Verksamt.se och 1177

[67] Den gemensamma infrastrukturen skulle kunna användas i ett byggblock eller utgöra ett eget byggblock i modellen, se https://www.digg.se/informationsutbyte-och-grunddata för rättslig PM och andra dokument.

[68] Artikel 5 EU:s dataskyddsförordning.

3.6 Överföring till tredje land

Personuppgiftsansvariga är skyldiga att säkerställa att uppgifter inte överförs till tredje land om det inte är tillåtet[69]. Av det som framkommit hittills är det inget som tyder på att uppgifter kommer att överföras till tredje land men frågan måste beaktas vid en eventuell utveckling av modellen då utkontraktering kan bli aktuellt i någon del.

[69] Jfr artikel 44-49 EU:s dataskyddsförordning

4 Särskilt om eget utrymme

Som framgått ovan är en teknisk lösning som innebär att information lämnas ut till individen själv på begäran, utifrån ett myndighetsperspektiv, den som är juridiskt hållbar både utifrån ett sekretessperspektiv, men även ett dataskyddsperspektiv. Det rekommenderas således att den tekniska lösningen stödjer ett sådant förfarande.

I detta sammanhang har ”eget utrymme” diskuterats. Ett eget utrymme kan beskrivas som en insynsskyddad elektronisk ”plats” hos en myndighet som bara individen ska ha tillgång till. Det är ett elektroniskt utrymme som en myndighet tillhandahåller en enskild. En myndighet ska inte, genom att tillhandahålla en sådan tjänst, ha insyn i de handlingar som finns i det egna utrymmet. Det får inte heller användas på ett sätt så att enskildas personliga förhållanden övervakas eller kartläggs[70]. Det egna utrymmet är alltså ett utrymme som myndigheten i och för sig tillhandahåller, men som myndigheten samtidigt inte får ha insyn i, och inte heller i vilket myndigheten har rätt att ta del av uppgifter.

Begreppet eget utrymme är typiskt sett kopplat till myndigheter och vissa utrymmen som tillhandahålls enskilda i myndighetens digitala sfär. Begreppet förekommer ibland även i relation till privata aktörer som tillhandahåller tjänster till enskilda. Redogörelsen nedan begränsas dock till att utgå från situationen för myndigheter.

4.1 Eget utrymme och allmänna handlingar

Eget utrymme tillhandahålls som en service åt individen. Individen kontrollerar utrymmet och de uppgifter och handlingar som finns häri och ingen annan ska få insyn i den information som finns där om inte individen tillåter det. Utrymmet är samtidigt tänkt att underlätta för användaren att skapa handlingar för att ge in i ärenden hos myndigheten, men det finns också utrymmen som ger annat stöd. Handlingar är individens egna handlingar och betraktas inte som inkomna och förvarade hos myndigheten om de inte aktivt ges in till myndigheten genom att individen skickar in dem från det egna utrymmet. Handlingar i det egna utrymmet blir därför inte allmänna enligt TF eller inkomna enligt förvaltningslagen så länge de finns i utrymmet och kriterierna för sådant utrymme är uppfyllda.[71]

[70] Eget utrymme hos myndigheten – en vägledning, eSams
[71] ibid

Frågan om eget utrymme och allmänna handlingar har prövats av kammarrätten i Stockholm[72]. Fråga var om handlingar i Arbetsförmedlingens (AF) CV-databas var allmänna. Kammarrätten konstaterade att CV-databasen var konstruerad som egna utrymmen för individer som vill lagra och skapa CV däri. CV-databasen var inte ett verksamhetssystem hos AF och informationen däri avsåg inte att ingå i myndighetens informationstillgångar. Uppgifterna användes inte heller av AF på något sätt, inte heller för framställning av statistik. Informationen användes inte i AF:s verksamhet. Mot bakgrund av dessa omständigheter ansåg kammarrätten att ett eget utrymme skulle liknas vid en plats för teknisk bearbetning och lagring för enskilds räkning, d.v.s. för annans räkning (jfr 2 kap. 9 § tredje stycket TF). Handlingarna i ett eget utrymme var således inte inkomna och förvarade till myndigheten och därmed inte allmänna.[73]

Utifrån uppdraget är det således ett möjligt tillvägagångssätt att genom egna utrymmen visa information till individen men också lämna ut information till individen. Det som finns däri är inte allmän handling och disponeras av individen ensam. Man skulle kunna likna det vid en digital brevlåda. Från utrymmet kan man sedan skapa möjligheter för individen att använda uppgifter och handlingar i olika sammanhang. Individen ska således kunna lämna in handlingar till olika myndigheter, och privata aktörer, från det egna utrymmet. Handlingarna blir inte inkomna till den eller de andra myndigheterna förrän individen vidtar en aktiv åtgärd för att tillgängliggöra informationen.

Utlämnandet sker således från en myndighet till individen som sedan får bestämma om informationen ska ges in till annan eller andra myndigheter eller privata aktörer. Ett sådant tillvägagångssätt är utifrån ett myndighetsperspektiv att förespråka med hänsyn till frågan om allmän handling och sekretess.

4.2 Eget utrymme och dataskydd

I avgörande från förvaltningsrätten i Stockholm var frågan bland annat om personuppgiftsansvaret för tjänsten Hälsa för mig som tillhandahålls av eHälsomyndigheten[74]. Hälsa för mig innehöll olika tjänster och vissa av dem

[72] Målnr 7369-15, dom meddelad den 26 oktober 2015

[73] Jfr även RÅ 1994 ref. 64 där fråga var om handlingar i ekonomisystem tillhandahållna av Riksrevisionen skulle anses inkomna dit. Se även HFD 2018 ref. 48, HFD 2013 ref. 86 och RÅ 1998 ref. 52 för frågan om inkomna handlingar samt RÅ 1998 ref. 30 och HFD 2011 ref 52 för frågan om upprättad handling. Se även prop. 1975/76:160 s, 87 och SOU 2014:39 s. 27-30 och 39-54

[74] Målnr 11458-17, dom meddelad 24 maj 2018

innebar att information behandlades i ett eget utrymme. eHälsomyndigheten framhöll att myndigheten inte har någon insyn eller kontroll i det egna utrymmet. Det är individen som fullt ut kontrollerar utrymmet och de uppgifter som samlas där och vilka som sprids. eHälsomyndigheten hänvisade också till att det inte skapas allmänna handlingar i ett eget utrymme eftersom de inte kan anses förvarade och inkomna till myndigheten så länge de ligger där.

Förvaltningsrätten konstaterade dock att det är myndigheten som utformar Hälsa för mig i syfte att uppfylla ett uppdrag och det är de som tillhandahåller plattformen genom ett personuppgiftsbiträde. Det är myndigheten som ingår avtal med de enskilda användarna av tjänsten, som avtalar med applikationsleverantörerna om möjligheten att få erbjuda applikationer och tillgång till uppgifterna i tjänsten. Det är myndigheten som bekostar tjänsten och som får betalning av applikationsleverantörema och det är myndigheten som tillhandahåller de tekniska förutsättningarna för att möjliggöra prenumerationstjänster. Eftersom det är E-hälsomyndigheten som bestämmer den yttre ramen för behandlingen av personuppgifter i tjänsten, är det myndigheten som bestämmer ändamålen med och medlen för tjänsten. E-hälsomyndigheten ansågs därför som personuppgiftsansvarig för de behandlingar av personuppgifter som sker i tjänsten som helhet. Även om de enskilda användarna av tjänsten hämtar uppgifter och kan dela uppgifter är det enbart E-hälsomyndigheten och dess personuppgiftsbiträden som behandlar uppgiftssamlingen som helhet. Att de registrerade användarna har en stor påverkan på tjänsten, och att uppgifterna hämtas från andra personuppgiftsansvariga, betyder inte enligt förvaltningsrätten att E-hälsomyndighetens personuppgiftsansvar minskas eller begränsas. Att den registrerade har samtyckt till behandlingen innebär inte heller att den personuppgiftsansvariges ansvar upphör.

Slutsatsen av domen är alltså att den myndighet som tillhandahåller ett eget utrymme är personuppgiftsansvarig för all den behandling som sker i utrymmet[75]. Ansvaret begränsas inte av att individen har en stor påverkan på vilka uppgifter som behandlas i det egna utrymmet eller vem uppgifter delas med. I och med den slutsatsen är det myndigheten som ensam behöver uppfylla kraven för de

[75] Se även HFD 2012 ref. 21 där Försäkringskassan ansågs som personuppgiftsansvarig för självbetjäningstjänster på dator eller i mobiltelefoner för anmälan av tillfällig föräldrapenning. Jfr dock med Integritetsskyddsmyndigheten (dåvarande Datainspektionen) beslut 2002-12-16 dnr 1682-2002. Se även diskussioner kring myndighetens personuppgiftsansvar för behandling i register av personer som inte är behöriga, SOU 2001:32 s. 105 samt prop. 2007/08: 126 s. 61.

behandlingar av personuppgifter som sker i ett eget utrymme. Detta inkluderar kravet på en rättslig grund för behandlingen och ett tillåtet ändamål. Betydelsen av detta utvecklas nedan.

4.3 Användningen av eget utrymme idag

Eget utrymme är ett utrymme som utvecklats i relation till regleringen i 2 kap. 9 och 13 §§ TF för att möjliggöra för enskilda att hos myndigheten förbereda handlingar i digitala tjänster som tillhandahålls den enskilda utifrån myndighetens verksamhet. Detta är en central förutsättning för behandlingen av uppgifter i det egna utrymmet. Eftersom myndigheten är personuppgiftsansvarig för det egna utrymmet ska myndigheten uppfylla samtliga grundläggande principer för behandling av personuppgifter som sker här[76]. Detta inkluderar principen om laglig grund och principen om ändamålsbegränsning. Eftersom dagens egna utrymmen i de allra flesta fall är direkt kopplade till myndigheternas verksamheter och de olika ärenden som handläggs så bör den behandling av uppgifter som sker i de egna utrymmena generellt sätt uppfylla principen om laglig grund och ändamålsbegränsning.

De uppgifter som behandlas i det egna utrymmet ska alltså vara behövliga för myndighetens verksamhet. Det innebär att det utifrån ett dataskyddsperspektiv inte är möjligt att i ett eget utrymme hos en särskild myndighet förvara och lagra uppgifter generellt utan koppling till myndighetens verksamhet.[77]

Användningen av eget utrymmet i modellen, för vilket syftet till största del är att tillhandahålla ett utrymme till vilket individen kan begära ut uppgifter och handlingar för att därefter skicka dem vidare, skiljer sig således till stor del från hur eget utrymme används idag. Man skulle kunna likna de egna utrymmena i modellen till brevlådor varifrån man skulle vilja ha möjligheten att skicka vidare uppgifter och handlingar. De rättsliga förutsättningarna för den behandling som skulle komma att ske i ett eget utrymme enligt modellen behöver därför utredas vidare utifrån de förutsättningar som gäller för att erbjuda individen insyn och kontroll enligt uppdraget. För detta syfte rekommenderas att möjligheterna för myndigheter att uppfylla de krav som åligger dem som personuppgiftsansvariga, samtidigt som de inte får ha insyn och rådighet över uppgifterna och handlingarna

[76] Artikel 5 EU:s dataskyddsförordning

[77] Jfr uppdragets slutsatser om serviceskyldigheten i 6 § FL och att denna inte såsom den kommer till uttryck idag kan användas som en rättslig grund för informationsutbytet i modellen, avsnitt 3.2.2.

i det egna utrymmet utifrån förutsättningarna för eget utrymme utifrån TF:s reglering, utreds vidare. En sådan utredning bör redogöra för hur myndigheter, utifrån tekniska förutsättningar, kan uppfylla kraven och förutsättningarna enligt båda regelverk för att möjliggöra användningen av eget utrymme för en ökad insyn och kontroll för individen.

5 Särskilt om indexering

5.1 Vad är indexering?

Indexering skulle kunna förklaras som en katalogisering av individer eller annat i en uppgiftssamling. Indexering innebär att metadata samlas in från de deltagande aktörernas uppgiftssamlingar. Indexering som begrepp är starkt kopplat till sökmotorer. Indexering i dessa fall är en process som resulterar i att en webbsida indexeras, det vill säga tas med i sökmotorns register över påträffade sidor på nätet. De olika söktjänsterna använder så kallade sökrobotar, eller ”spindlar” för att upptäcka nya sidor på webben och för att hämta information om dem. Resultatet samlas därefter i sökmotorns index. Indexeringen påverkar således träfflistan för den som använder sökmotorn.

Indexering så som det beskrivs ovan med sökspindlar som letar information, utgår från att ett index samlar in information genom att uppgifter lämnas ut från de deltagande aktörerna till indexet efter en begäran. Efter detta lagrar indexet uppgifter om vilken information uppgiftssamlingen innehåller. När någon därefter söker i indexet presenteras resultatet av indexeringen.

Indexering kan också fungera så att data lämnas ut till ett index från olika aktörer på eget initiativ. Indexet begär i detta fall inte ut uppgifter. Om dataöversikten, exempelvis, har ett index kan det alltså istället fungera så att uppgifter lämnas ut till indexet från anslutna aktörer på eget initiativ. Det kan ske genom avisering, d.v.s. att aktörerna skickar en signal om att nya data finns att hämta. Ett index behöver i dessa fall alltså inte leta eller fråga efter information.

5.2 Indexering i modellen

Indexering som funktion skulle kunna bli aktuell när det gäller insynsdelen i uppdraget. Tanken har varit att insynsdelen kommer att finnas i dataöversikten i modellen. Här ska individen kunna se vilka uppgifter som olika aktörer behandlar om hen. Uppgifterna behöver presenteras på ett överskådligt, begripbart och strukturerat sätt för individen[78]. Detta kan ske på olika sätt. En sektorsvis presentation, d.v.s. att uppgifter inom en viss sektor, exempelvis hälsa och sjukvård eller utbildning presenteras samlat, skulle kunna vara ett alternativ. Hur uppgifterna ska presenteras i insynsdelen har dock inte diskuterats i uppdraget. Oavsett kommer indexering att aktualiseras för en bättre presentation av uppgifter

[78] Jfr kraven på tydlighet m.m. i artikel 12 EU:s dataskyddsförordning

i insynsdelen såsom modellen är tänkt. Huruvida indexeringen kommer att ske genom att uppgifter hämtas av ett index eller om aktörerna självmant ska skicka information till indexet har inte diskuterats.

5.3 De rättsliga aspekterna av indexering

Indexering innebär en behandling av personuppgifter i sig. Som modellen har beskrivits är indexering aktuell i dataöversikten hos ekosystemansvarig i dataöversikten. Med detta som utgångspunkt blir den som är personuppgiftsansvarig för ekosystemansvarig eller dataöversikten i modellen personuppgiftsansvarig även för den behandlingen som indexeringen innebär.

Som framgår ovan ska all behandling uppfylla kraven enligt de grundläggande dataskyddsprinciperna[79]. Indexeringen i modellen innebär att metadata kommer att lämnas ut från deltagande aktörer till den part som ansvarar för indexet. Behandlingen som utlämnandet innebär behöver uppfylla de grundläggande principerna för personuppgiftsbehandling, bland annat de om laglig grund och tillåtet ändamål. I detta avseende är det viktigt att klargöra vem som agerar, alltså om uppgifterna lämnas ut efter en begäran eller på eget initiativ. Även den grundläggande principen om lämplig säkerhet för behandlingen[80], såsom exempelvis spårbarheten, behöver också säkerställas mellan deltagande aktörer och indexet. Indexet behöver också ha behörighetsinformation i detta avseende. Det måste finnas information i indexet som talar om vem som får ta del av/använda indexet som pekare mot vart informationen finns.

Ett index kan vidare vara smalt eller brett. Ju bredare indexet är desto mer omfattande blir behandlingen. Ju bredare ett index blir ju större blir också behovet av att i indexet ha parametrar som katalogiserar karaktären av den information som indexet pekar mot. I det fall modellen innebär att allas samtliga uppgifter ska kunna visas måste indexet kunna särskilja vårduppgifter, utbildningsuppgifter, skatter o.s.v. Om man inte har en sådan katalogisering kommer den enskilde att bli översköljd av uppgifter som presenteras vilket rimligen leder till en dålig användarupplevelse. Dessutom innebär en bristande katalogisering att om den enskilde bara vill veta vilka utbildningsuppgifter som finns men istället får se all information som inhämtats att mycket mer information än vad som egentligen

[79] Artikel 5 EU:s dataskyddsförordning
[80] Jfr artikel 5 1. f och 32 EU:s dataskyddsförordning

efterfrågas kommer att behandlas. Detta är inte förenligt med principen om uppgiftsminimering[81].

Utifrån ett sekretessperspektiv innebär utlämnandet av uppgifter från aktörer som är offentliga att detta kan hindras av att sekretess gäller för uppgifterna. Om uppgifterna omfattas av sekretess krävs en sekretessbrytande bestämmelse eller ett undantag från sekretess för möjligheten att lämna ut uppgifter till indexet. En annan fråga utifrån ett sekretessperspektiv är den om sekretesskyddet för de uppgifter som kommer att finnas i indexet. Den frågan kräver utredning om det ska säkerställas att uppgiftssamlingen ska kunna skyddas mot insyn om indexet finns hos en offentlig aktör. Det kan konstateras att om nuvarande sekretessreglering inte erbjuder ett skydd för uppgifterna kommer uppgiftssamlingen att bli en källa för information till tredje part.

Det breda indexet är i sig själv ett problem. Det riskerar att bli en stor informationssamling som riskerar integriteten hos de registrerade personerna och som kan vara svår att skydda mot insyn enligt resonemanget ovan. Det finns därför anledning att hålla indexen smala. Utifrån ett integritetsperspektiv bör det vara lättare att skapa uppdrag och legalitet för smala index. Hur indexen i slutändan utformas måste dock utredas vidare och övervägas noggrant i samband med att modellen eventuellt utvecklas.

[81] Artikel 5 p. 1 c EU:s dataskyddsförordning