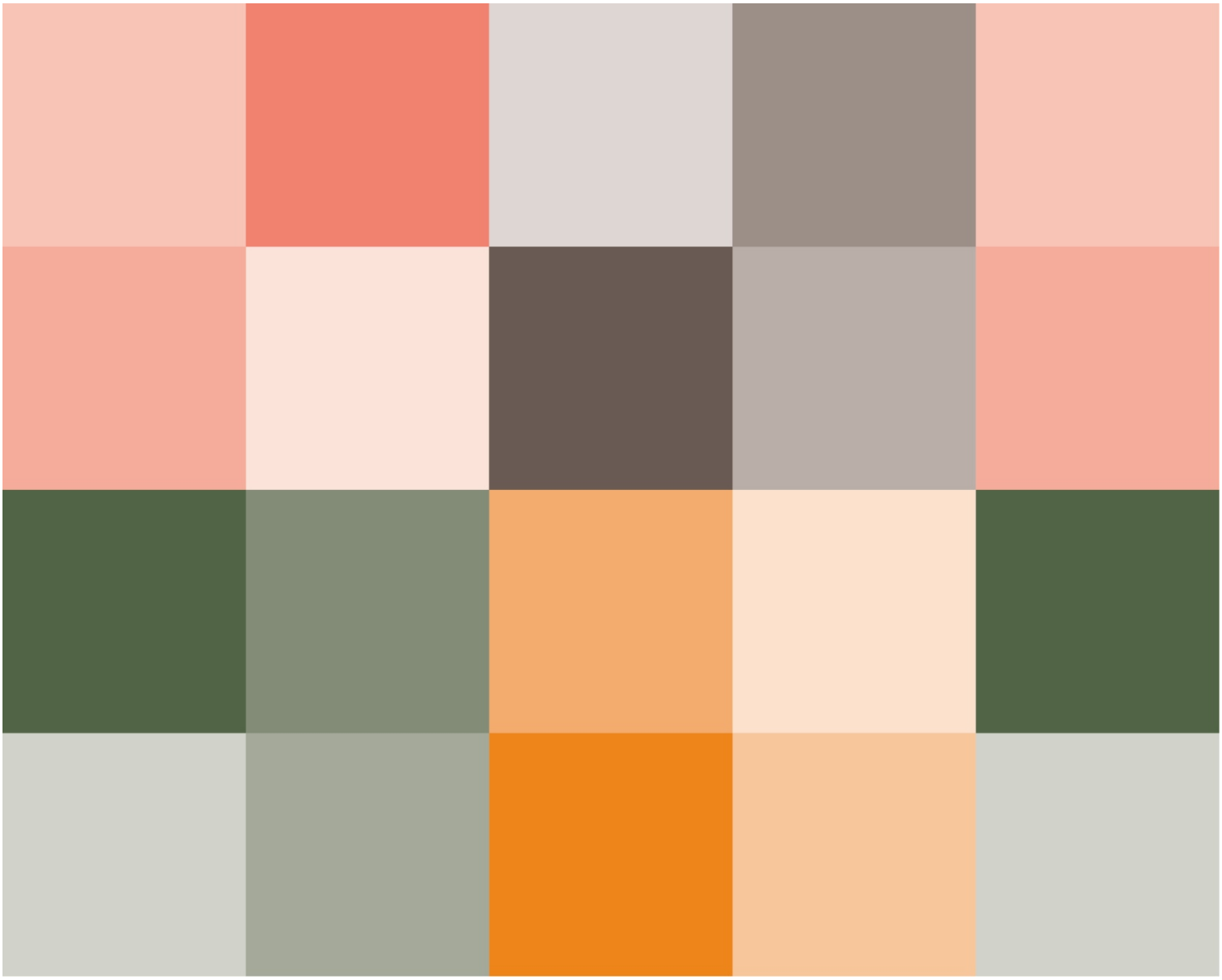


Uppdrag att möjliggöra lösningar för individen till kontroll och insyn av data om individen

I2020/02024/DF

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Förord

I juli 2020 fick Arbetsförmedlingen, E-hälsomyndigheten, Myndigheten för digital förvaltning (DIGG) och Skatteverket i uppdrag att gemensamt visa hur individens möjligheter till insyn och kontroll över de data om individen som finns hos offentlig sektor, och i förlängningen även de data om individen som finns hos privat sektor, kan öka.

DIGG har ansvarat för den övergripande samordningen av uppdraget. Arbetsförmedlingen har ansvarat för utvecklingen av koncepttestet. Arbetet med föreliggande rapport har genomförts gemensamt och därför används ”vi-formen” i rapporten.

Till uppdraget har en myndighetsgemensam styrgrupp varit knuten. Styrgruppen har bestått av följande personer. Från E-hälsomyndigheten har rättschef Erik Janzon deltagit fram till 2021-03-01 då rättschef Maria Jacobsson tog över. Från DIGG har leveransledare Viktoria Hagelstedt deltagit fram till 2021-02-01 då leveransområdeschef Mats Snäll tog över. Från Skatteverket har Andreas Elvén deltagit och från Arbetsförmedlingen har Gregory Golding deltagit.

Beslut om denna rapport har fattats av generaldirektörerna för respektive myndighet. För E-hälsomyndigheten Janna Valik, för Skatteverket Katrin Westling Palm, för DIGG Anna Eriksson och för Arbetsförmedlingen Maria Mindhammar.

Theodor Andersson, DIGG, Jan Sjösten, Skatteverket, Hans Ahlqvist, Arbetsförmedlingen och Bessam Saleh, E-hälsomyndigheten har varit föredragande.

Stockholm den 1 juni 2021

Sammanfattning

Arbetsförmedlingen, E-hälsomyndigheten, Myndigheten för digital förvaltning (DIGG) och Skatteverket har fått regeringens uppdrag att undersöka förutsättningarna för hur individens möjligheter till insyn och kontroll över de data om individen som finns hos offentlig sektor, och i förlängningen även de data om individen som finns hos privat sektor, kan öka.

Vem som har kontroll över individens data kommer att få allt större betydelse i samhället framöver. Digitaliseringen av Sveriges offentliga sektor har länge utgått från respektive myndighets behov, där stora delar av den digitala utvecklingen motiverats med ökad effektivitet och produktivitet. Därefter präglades det offentliga i allt större utsträckning av satsningar som prioriterar individers behov av enkel, snabb och tillgänglig service. Det är en viktig utveckling men inte tillräcklig eftersom satsningarna till stor del utgått från den egna verksamheten och det ansvar som respektive myndighet har. Den senaste utvecklingen är att tjänsterna utgår utifrån så kallade livshändelser som individer går igenom i olika skeden av livet. På så sätt kan det offentliga ge invånarna mer sammanhållna, individcentrerade och integrerade tjänster som spänner över myndighets- och sektorsgränser. Denna utveckling, som drivs på genom olika initiativ i form av policydokument och strategier på såväl nationell nivå som från EU, aktualiserar nya behov, möjligheter men också utmaningar.

För att lyckas leverera samhällstjänster som motsvarar dagens och framtidens förväntningar från invånarna blir det allt mer uppenbart att data behöver ses som en strategisk resurs. De nordiska ländernas, inte minst Sveriges, dataregister är inte bara unika för att de funnits så länge, de är också unika för att olika myndigheter har stöd i sin nationella lagstiftning för att samla in och underhålla en stor mängd uppgifter. Detta har skapat goda förutsättningar för en datadriven förvaltning som kan använda relevant data när de behövs – givet att integritets- och säkerhetskrav är uppfyllda.

Genom att ge individer ökad insyn och kontroll om uppgifter som finns om dem, i såväl offentlig som privat sektor, kan skapa stora ekonomiska och andra värden. Företag och organisationer skulle med hjälp av data som individen kontrollerar kunna skapa innovativa tjänster till invånarna och andra företag, och på så sätt bidra till att utveckla den svenska ”data-ekonomin”.

För att myndigheterna ska kunna fortsätta leverera nya tjänster som lever upp till invånarnas ökade förväntningar behöver nya förutsättningar skapas. Dataöverföringen, som utgör kärnan i de moderna tjänsterna, behöver en infrastruktur som kan binda samman olika sektorer. Det är viktigt att arbetet med den förvaltningsgemensamma digitala infrastrukturen kan utvecklas för att också möta individers behov av insyn och kontroll. Om datadelningen i framtiden i allt större utsträckning kommer att använda samtycke som legal grund för personuppgiftsbehandlingen kommer också den digitala kompetensen hos invånarna att bli en viktig förutsättning. För att behålla tilliten till det offentliga, och i förlängningen till de privata företagen som hanterar stora mängder personliga data, blir frågor om insyn och kontroll – det vill säga hur och av vem data används – allt viktigare.

Omvärldsanalysen har stärkt bilden av att individens ökade insyn och kontroll över personliga data är ett prioriterat område inte bara för Sverige utan för många länder. Därför försöker EU och allt fler medlemsländer hitta nya möjligheter att ge invånarna inflytande över sina personliga data. För att lyckas krävs att tekniska lösningar kombineras med juridiska ramverk, sekretess- och integritetsskydd som stödjer en sådan utveckling. Det är även viktigt att invånarna förstår betydelsen av dataskydd och har tillräcklig digital kompetens att agera på de möjligheter som finns för att skydda de personliga data som finns om dem hos olika aktörer. Vår omvärldsanalys visar att inget enskilt land, varken inom eller utanför EU, har lyckats fullt ut.

Vi har tagit fram ett koncepttest (PoC) som visar hur en individ kan hämta data från några myndigheter för att hos Arbetsförmedlingen kunna skapa ett CV med validerade uppgifter från olika källor som kan användas för att underlätta arbetssökande. Detta skapar en trovärdighet för uppgifterna och skapar förutsättningar för individer att effektivera sin ansökningsprocess. Vi ser att lösningsförslagen i koncepttestet skapar förutsättningar för och visar hur möjlighet till insyn och kontroll över data om individen hos offentlig sektor, och i förlängningen privat, kan ge tydliga mervärden för individen och i detta fall underlätta sitt arbetssökande.

I syfte att försöka flytta fram den svenska positionen när det gäller individens ökade möjligheter till insyn och kontroll av personliga data presenterar vi en modell som visar hur ett förvaltningsgemensamt dataekosystem skulle kunna utformas. Den visar hur framtidens dataflöden, som under kontroll och insyn av

individen, skulle kunna bidra till ökad effektivitet, individcentrering och innovation. Modellen är konceptuell vilket innebär att flera förutsättningar behöver tillkomma eller förändras. För att konkretiska de framtida möjligheterna har vi tagit fram en visualisering av en hypotetisk framtida tjänst som ska möta individers behov i livshändelsen *bli sjukskriven.*

Under arbetet med detta regeringsuppdrag har vi uppmärksammat flera rättsliga utmaningar som behöver utredas vidare innan tankar som ekosystem, insyn och kontroll kan bli verklighet. Det finns en potentiell motsättning mellan å ena sidan den enskildes rätt till insyn och kontroll och å andra sidan myndigheters förutsättningar att realisera sådan insyn och kontroll.

Det är inte helt självklart hur Sveriges invånare vill att insyn och kontroll över data ska komma till utryck. Vi föreslår därför att en invånarundersökning genomförs för att närmare undersöka hur verktyg för insyn och kontroll kan utformas som också är digitalt inkluderande.

Den konceptuella modell som presenteras i denna rapport bedömer vi kan vila på den förvaltningsgemensamma digitala infrastrukturen som nu växer fram.[1] Vi bedömer att byggblocken Mina ombud, Mina ärenden och Min profil kan skapa förutsättningar för den dataöversikt som vi anser behövs. Även byggblocket Indexering är en viktig förutsättning i det fortsatta arbetet. Frågan om individers insyn och kontroll kan därför med fördel utvecklas vidare inom den förvaltningsgemensamma digitala infrastrukturen.

Så kallat eget utrymme hos myndighet används idag av myndigheter för att ge service åt invånare och företag. Flera rättsfrågor om förutsättningarna att använda eget utrymme för att tillgodose ökad insyn och kontroll är idag outredda. Vi rekommenderar därför att dessa utreds vidare. En viktig del i ett sådant arbete är att undersöka de rättsliga förutsättningarna och begränsningarna avseende personuppgiftsansvarets räckvidd i förhållande till eget utrymme. En annan viktig del är att utreda hur eget utrymme kan utformas i syfte att stödja en individcentrerad datadelning inom sektorer eller livshändelser. Detta arbete kan lämpligen göras i samråd med Integritetsskyddsmyndigheten i syfte att

[1] Regeringen (2019) *Uppdrag att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte* Dnr I2019/03306/DF

åstadkomma ett proaktivt förhållningssätt och i ett tidigare skede uppmärksamma behov av att anpassa regelverk.

Idag regleras myndigheters behandling av personuppgifter genom sektorspecifik lagstiftning. Den rättsliga statusen för digitala informationsöverföringar och möjligheter att ge individen insyn och kontroll får anses som osäker. Vi föreslår därför att en konsekvensanalys av en utvidgning av serviceskyldigheten genomförs tillsammans med en översyn av den särskilda dataskyddsregleringen (registerlagar) och möjligheten att lämna ut uppgifter i elektronisk form.

Innehållsförteckning

1 Inledning

1.1 Bakgrund

Offentlig förvaltning behandlar stora mängder data om individer vilket de har stöd för i författningar eller avtal. Ofta har offentlig sektor inte bara en rätt utan också en skyldighet att behandla data om individen.

EU:s dataskyddsförordning (GDPR) gäller för alla organisationer och branscher som hanterar personlig och känslig information om individer. Den ger individer rättigheter att bland annat rätt att få ut ett registerutdrag, det vill säga information om vilka personuppgifter som behandlas och på vilket sätt de behandlas, liksom rätt att begära att personuppgifter raderas eller att data överförs från en aktör till en annan (dataportabilitet). För individen kan det dock upplevas som svårt att överblicka och få insyn i den information som olika aktörer har om individen. I många fall har individen begränsade möjligheter att på ett enkelt sätt digitalt påvisa felaktiga data eller att begära att data från olika aktörer ska raderas.

Att kunna återanvända uppgifter som redan finns hos en myndighet som underlag för beslut eller åtgärder hos en annan aktör skulle förenkla för individer och skapa effektiviseringar för offentlig sektor. Men hur det ska gå till och vilka förutsättningar som behöver finnas på plats för en sådan individcentrering är oklart. I detta uppdrag har vi utforskat hinder och möjligheter till att förbättra och underlätta individers insyn i, och kontroll över, över data som finns om individen hos offentlig sektor.

1.2 Uppdraget

Regeringen har gett Arbetsförmedlingen, E-hälsomyndigheten, Myndigheten för digital förvaltning (DIGG) och Skatteverket i uppdrag att genomföra en omvärldsanalys och ta fram ett koncepttest (eng. *Proof of Concept*, PoC) som visar hur det är möjligt att öka individens möjligheter till insyn och kontroll över de data om individen som finns hos offentlig sektor, och i förlängningen även de data om individen som finns hos privat sektor.[2]

[2] https://www.regeringen.se/4a647d/contentassets/84872b67c0c8480a9544dc076fa20aef/uppdrag-att-mojliggora-losningar-for-individen-till-kontroll-och-insyn-av-data-om-individen.pdf

1.3 Disposition av rapporten

Rapporten består av sju kapitel. Inledningen består av rekommendationer till fortsatt utredning och en beskrivning av hur uppdraget har genomförts. Kapitel 2 består av en genomförd behovsanalys som bland annat belyser medborgerliga attityder till delning av data och ett ökat individuellt ansvar för detta. Kapitel 3 beskriver utvecklingen i omvärlden. Det handlar dels om arbete som pågår inom EU, FN och OECD-nivå, dels insikter från initiativ och projekt som genomförts eller pågår i andra länder. I kapitel 4 redogörs kort för den förvaltningsgemensamma digitala infrastruktur för informationsutbyte som nu växer fram i Sverige. Dessutom beskrivs tankarna bakom digitala ekosystem och exempel på hur vissa tjänster idag ger insyn och kontroll. I kapitel 5 presenteras det koncepttest som Arbetsförmedlingen fått i uppdrag att utveckla inom ramen för detta uppdrag. I kapitel 6 beskrives en förvaltningsgemensam modell för hur individen kan få insyn och kontroll. över data om sig själv samt hur modellen kan appliceras på en livshändelse i syfte att underlätta individens kontakter med offentliga och privata aktörer. Avslutningsvis, i kapitel 7 pekar vi på de behov som behöver adresseras och gör ett antal rekommendationer för vidare arbete.

Till denna rapport finns fyra bilagor. Syftet med uppdelningen är att skapa en komprimerad huvudrapport som lyfter fram centrala aspekter från till exempel omvärldsanalysen och inhemska erfarenhetsutbyten. Bilaga 1 innehåller underlaget för behovsanalysen som består av granskning av ett antal svenska och utländska medborgarundersökningar. Bilaga 2 består av omvärldsbevakningen av EU, FN och OECD samt av sju länder som analyserats inom ramen för uppdraget. Bilaga 3 är ett samlat dokument innehållande en utförlig juridisk analys och Bilaga 4 är en mer utförlig och teknisk beskrivning av det tekniska koncepttestet som utvecklats under Arbetsförmedlingens ledning.

1.4 Uppdragets genomförande

DIGG har ansvarat för den övergripande samordningen av uppdraget och Arbetsförmedlingen har ansvarat för utvecklingen av koncepttestet. I övrigt har uppdraget bedrivits i samarbete och i samverkan mellan myndigheterna.

I den inledande delen av omvärldsbevakningen granskades olika rapporter, strategier och andra publikationer från EU, FN och OECD för att fastställa om det råder konsensus kring frågan om huruvida individen har en rättighet till ökad insyn och kontroll över data om individen och hur väl den teknologiska

utvecklingen samt diskussioner om policy, ledning och styrning sammanfaller med visionen för hur denna insyn och kontroll ska ges till och hanteras av individen.

Vidare analyserades exempel från ett antal olika länder (Finland, Frankrike, Norge, Danmark, USA, Storbritannien och Indien) för att lyfta fram olika aspekter av insyn och kontroll såsom tekniska lösningar, juridiska aspekter, näringslivets involvering och värdet av politisk styrning.

En representant från respektive myndighet har utgjort en styrgrupp som haft möjlighet att ta del av arbetets löpande utveckling genom återkommande möten och avstämningar. Styrgruppen har haft mandat att fatta beslut som lyfts av arbetsgruppen och att själva lämna rekommendationer för arbetets utformning och inriktning.

För att organisera arbetet med uppdraget skapades även ett antal särskilda arbetsgrupper som haft specifika fokusområden och som stämt av sitt arbete löpande med den övergripande arbetsgruppen för uppdraget.

1.4.1 Arbetet med juridik

De rättsliga aspekterna har utgjort ett särskilt fokusområde för uppdraget och en särskild arbetsgrupp skapades med jurister från de samverkande myndigheterna inom uppdraget. De juridiska diskussionerna som gruppen har ägnat sig åt har utgått från uppdragets arbete med att ta fram en generisk modell samt de livshändelser som har använts för framtagande av koncepttesten och den informationsdelning som dessa innebär.

Arbetsgruppens arbete redovisas i sin helhet i Bilaga 3 *Övergripande juridisk analys av möjligheten att öka insynen och kontrollen för individer*. De slutsatser som arbetsgruppen gjort i sin analys av den rättsliga regleringen och de begränsningar respektive möjligheter som den ger för att dela information enligt den konceptuella modellen, har beaktats i arbetet med att skapa koncepttestet.

Förutom den övergripande analysen som redovisas i Bilaga 3, finns en särskild juridisk analys av det tekniska koncepttestet (livshändelsen *gå till arbete*) som Arbetsförmedlingen har ansvarat för. Den juridiska analysen som redovisas i anslutning till det koncepttestet är förankrad i den allmänna juridiska analysen som görs i Bilaga 3.

1.4.2 Arbetet med livshändelser

För att förstå individers behov och hitta utvecklingsområden som kan förenkla vardagen för många är det viktigt att utgå från ett livshändelseperspektiv. Därför skapade vi arbetsgruppen *livshändelser,* som har nyttjat eSams[3] arbete kring hur myndigheter kan arbeta utifrån medborgarens livssituation.[4] Exempel på kategorier i en livssituation är hälsa, arbete och utbildning. I en individs livssituation inträffar händelser som påverkar livssituationen och dessa kallas för livshändelser. Exempel på livshändelser kan till exempel vara att *bli sjukskriven*, som då är knuten till livssituationen *hälsa*, *gå till arbete* som är knuten till livssituationen *arbete* och så vidare.

Arbetsgruppen har fokuserat på två livshändelser, g*å till arbete* och *bli sjukskriven*, vilka möjliggör för en nödvändning avgränsning av mängden och typ av data som inkluderas i analysen. Delningsmoment av data och antalet involverade aktörer har avgränsats för att underlätta analysen.

När en livshändelse inträffar gör medborgaren något, det benämns agerande i rapporten. Exempel på ageranden i livshändelsen *bli sjukskriven* kan vara *kontakta vården*, och i *söka jobb* är agerandet kopplat till livshändelsen *gå till arbete* I livshändelseanalysen har behoven varit vägledande och inte myndigheternas uppdrag eller organisatoriska strukturer. Målet är att förenkla för individen.

Livshändelserna *gå till arbete* och *bli sjukskriven* har valts utifrån följande dimensioner:

- förvaltnings- och sektoröverskridande
- skapar stort mervärde för individen
- insyn och kontroll ska kunna appliceras på andra livssituationer och livshändelser.

Arbetet med livshändelsen *bli sjukskriven,* resulterade i en visualisering som illustrerar ett framtidsscenario och innehåller ingen teknisk funktionalitet. Den konceptuella modell för ett individcentrerat dataekosystem som utarbetats som en

[3] eSam är ett medlemsdrivet program för samverkan mellan 29 myndigheter och SKR där ett centralt mål är att underlätta privatpersoners och företagens behov av att utföra olika ärenden hos myndigheter och kommuner

[4] eSam (2016) *Behovsdriven utveckling – en vägledning.*

del av regeringsuppdraget ligger till grund för det framtidsscenario som i rapporten beskrivs som *nyläge*.

Arbetet med livshändelsen *gå till arbete* ligger till grund för det koncepttest som beskrivs i följande avsnitt.

1.4.3 Arbetet med koncepttest (Proof of Concept – PoC)

En arbetsgrupp har tagit fram ett koncepttest (PoC) som visar hur ökad möjlighet till insyn och kontroll över data om individen hos offentlig, och i förlängningen, privat sektor kan ge tydliga mervärden för individen. Integritet och dataportabilitet utgör kärnan i uppdraget, och därmed också de juridiska förutsättningarna för att hantera och dela personliga data.

Arbetsförmedlingen har ansvarat för genomförande och leverans av det tekniska koncepttestet av livshändelsen *gå till arbete*.

1.5 Avgränsningar

Livshändelser Val av livshändelser har fokuserat på hälso- och arbetsmarknadsrelaterade händelser. Detta är två högprioriterade områden för just delning av data eftersom det finns stora samhällsekonomiska vinningar att göra. Dessutom, i tider av pandemi, är dessa två områden högaktuella eftersom både hälsosektorn och arbetsmarknaden blivit hårt ansatta av pandemins konsekvenser för människors möjlighet till god hälsa och till trygga anställningsvillkor. Livshändelserna har kortats ner till specifika moment inom större livshändelser.

Kontakter med näringsliv I uppdraget ingår för myndigheterna att resonera kring möjligheterna att möjliggöra för individen att med digitala verktyg få ökad kontroll och insyn i de data om individen som finns hos privat sektor och att därför föra dialog med relevanta privata aktörer. Det primära fokuset har dock varit på offentlig förvaltning och merparten av konsultationer med externa aktörer har hanterats inom arbetet med att utveckla konceptestet för livshändelsen att *gå till arbete.*

Avgränsningar i antalet kontakter med privata aktörer och antal områden som utretts har berott på komplexiteten i uppdraget. Det har därför gjorts ett aktivt val genom att prioritera offentlig förvaltnings roll i ett individcentrerat digitalt ekosystem. Det finns ett behov av fortsatt arbete med öppnare och bredare kontakt med näringslivet men då juridiska restriktioner och möjligheter först klargjorts. Det har framkommit av omvärldsanalysen att näringslivets medverkan

kommer till bäst användning då offentliga aktörer bättre förstår möjliga implikationer av de lösningar som föreslås för företag och deras hantering av kunddata. Det är även önskvärt med tydliga juridiska förutsättningar och miljöer för experimentellt innovationsarbete såsom till exempel regulatoriska sandlådor eller växthus.

1.6 Centrala begrepp

Det finns tre begrepp som är centrala i rapporten och dessa är insyn, kontroll och personliga data eller personuppgifter. Även termen individcentrerad förekommer på flertalet ställen och definieras därmed nedan. Andra centrala begrepp som nyttjas för att förklara olika delar av den konceptuella modell för individens insyn och kontroll som beskrivs i kapitel 6 återges i anslutning till det stycket och i synnerhet i avsnitten 6.1.1 – 6.1.3.

Insyn Med insyn avses i detta uppdrag att individen på ett lättöverskådligt och samlat sätt ska kunna visualisera eller på annat sätt förstå vilken typ av data som finns om individen, hos vilken organisation data finns och för vilka ändamål de samlas in samt på vilken legal grund de behandlas där.

Kontroll Med kontroll avses i huvudsak digitala möjligheter att för individen begära ut, begära rättelse, radering och begära överföring av data till och från den aktör som har den.

Personliga data och personuppgifter Personuppgifter är all information som rör en identifierad eller identifierbar levande enskild person. Olika uppgifter som tillsammans kan leda till att en viss person kan identifieras, utgör också personuppgifter. Det kan vara identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Individcentrerad Individcentrerad innebär att tjänster utgår från individers behov och låter individer vara mer delaktiga i processerna.

2 Erfarenheter från behovsanalys

Syftet med att genomföra en analys av uppfattningar hos privatpersoner om hur data om individen hanteras och delas, av såväl offentliga och privata aktörer, ansågs viktig att inkludera i detta uppdrag. Det saknas ofta ett medborgarperspektiv även om det är den enskilde medborgaren som förväntas ta ett större personligt ansvar för data om hen själv och för data som genereras av individens digitala interaktion med offentliga och privata aktörer. För mer detaljerad genomgång se bilaga 1 *Behovsanalys och medborgarperspektiv*.

2.1 Summering och erfarenheter från behovsanalysen

- Integritetsparadoxen betyder att ökad insyn inte nödvändigtvis leder till ändrat beteende hos dem som anger att de är oroade över att de inte har insyn eller kontroll över hur deras personliga data nyttjas.
- De flesta medborgarundersökningar visar att det offentliga har en viktig roll att spela vad det gäller att ge legitimitet till nya metoder för datadelning och användning. Tillit till det offentliga är en viktig aspekt för hur medborgare ser på att ingå i ett datadelningsekosystem som även inkluderar privata företag.
- Ökad kontroll över egna personliga data är generellt sätt önskvärt men få har insikter i hur denna kontroll kan nyttjas eller om man vill ta på sig ett ökat ansvar för delning av data som är nödvändig för effektiva offentliga tjänster.
- Beräkningar från Storbritannien visar att det finns ett stort potentiellt ekonomiskt värde av en omställning mot ökad dataportabilitet. Denna del av behovsanalysen behöver utredas mer utifrån svenska förutsättningar och möjligheter. Individers och organisationers vilja att betala för de tjänster som en leverantör av ”personal information management systems” (PIMS) kan erbjuda behöver kvantifieras.

2.2 Kort om tillit, attityder och dataskydd

Två händelser de senaste åren kan ses som särskilt betydande för diskussionen om hantering av personliga uppgifter på nätet. Den första är dataskyddsförordningen

(GDPR) som trädde i kraft 2018. Den andra är händelsen kring företaget Cambridge Analytica som samlat in miljontals Facebooks-användares personliga information i syfte att påverka utgången av det amerikanska presidentvalet 2016. Dessa händelser har väckt frågan om vad individen är villig att godkänna i termer av hur personliga data samlas in, används och säljs vidare av privata företag i utbyte mot tillgång till deras digitala tjänster.

Hur organisationer använder personuppgifter påverkar människors förtroende till dem. Kort tid efter Cambridge Analytica händelsen genomförde Novus en undersökning där var tredje svensk uppgav att de skulle ändra sitt beteende, exempelvis genom att sluta göra personlighetstester eller frågesporter på Facebook. En lika stor andel funderade på att lämna Facebook helt, men väldigt få gjorde verklighet av saken.[5] Generellt är människor oroliga för sin personliga integritet men samtidigt tar de sällan nödvändiga åtgärder för att skydda sina personuppgifter. Detta glapp mellan attityd och faktiskt beteende kallas *integritetsparadoxen*. Insyn i hur personuppgifter används behöver enligt denna paradox inte nödvändigtvis leda till ändrat beteende även om människor är oroade över att de inte har någon kontroll över data om sig själv och hur den används. Enligt undersökningen *Delade meningar*[6] har till exempel endast 4 procent av de medverkande bett om att få tillgång till sin personliga information.

Det finns tydliga geografiska skillnader mellan olika delar av världen när det gäller tillit till att personliga data inte ska missbrukas. Enligt rapporten The Global State of Online Digital Trust har människor i Europa en betydligt lägre grad av tillit till att deras personuppgifter inte missbrukas av företag jämfört med resten av världen.[7] Tilliten har dessutom minskat över tid. En förklaring som lyft fram i rapporten kan vara att de europeiska lagar som syftar till att värna individens grundläggande rättigheter upplevs som hotade av de företag som i allt större utsträckning använder personuppgifter i olika syften. Samtidigt som människor har relativt låg tillit till företagens hantering av personliga data, föreställer sig allt fler företag att deras digitala förtroendekapital har ökat. Konsumenters tillit till

[5] SVT (2018) *Svenskarnas förtroende för Facebook rasar* Publicerad 2018-03-29

[6] Delade meningar, svenska folkets attityder till digital integritet 2020 deladeMeningar2020_Web_1-9A.pdf (insightintelligence.se)

[7] https://docs.broadcom.com/doc/the-global-state-of-online-digital-trust

företagens hantering av personliga uppgifter behöver förbättras om företagen avser att växa.

Hur privata företag hanterar personliga data är det som främst oroar svenskar och den generella oron för att data används i syften som man inte godkänt eller har insyn i har dubblerats mellan 2015 – 2020. Idag delar 49 procent av befolkningen den oron.[8] Känslan av trygghet ökar inte heller nödvändigtvis om personliga data avidentifieras eftersom företagen då inte är skyldiga att berätta hur den används. Trots att de flesta tillfrågade har en relativ hög tillit till hur statliga aktörer hanterar data om individen så upplever en klar majoritet att delning av data sker utifrån tvång snarare än frivillighet.

OECD identifierar tillit till staten som en viktig faktor och avgörande för hur medborgares attityd till datahantering ter sig. Lyhördhet, handlingskraft och tillförlitlighet när det gäller att tillhandahålla offentliga tjänster och förutse nya behov är avgörande för att öka förtroendet för institutionerna.[9] I detta avseende är Sverige ett så kallat högtillitssamhälle. Traditionellt sett har förtroendet för och tilliten till det offentliga haft tydliga kopplingar till hur väl skola, vård och omsorg upplevs fungera. I en tid av digital transformation är även förmågan att kunna leverera väl fungerande, säkra, pålitliga och transparenta digitala tjänster en betydande bidragande faktor för tillit till en offentlig aktör. För att behålla medborgarnas tillit är det centralt hur offentlig sektor hanterar medborgarnas data. Detta konstaterar Integritetsskyddsmyndigheten i sin Integritetsskyddsrapport 2020[10] där man även bedömer att detta regeringsuppdrag att möjliggöra lösningar för individen till kontroll och insyn av data om individen sannolikt behöver åtföljas av fler uppföljande uppdrag eller utredningar för att stärka enskilda individers möjligheter att kontrollera egna data.

2.3 Mönster i medborgarundersökningar

Det är inte självklart att kontroll över personliga data ökar individers egenmakt i relation till offentliga och privata aktörer. Om individer ökar sitt ansvarstagande för datahantering kan en känsla av hopplöshet infinna sig. Denna ”digitala uppgivenhet” uppstår då man inte tror att offentliga eller privata aktörer kommer

[8] Delade meningar, svenska folkets attityder till digital integritet 2020 deladeMeningar2020_Web_1-9A.pdf (insightintelligence.se)
[9] https://media.sitra.fi/2020/10/08100935/towards-trustworthy-health-data-ecosystems.pdf sid.18
[10] https://www.imy.se/globalassets/dokument/rapporter/integritetsskyddsrapport2020.pdf

att ändra sin hantering av data oavsett den enskildes agerande. Den enskildes handlingsutrymme upplevs även som mycket begränsad då en majoritet upplever att man delar information främst för att man tvingas att göra det.[11]

En slutsats som kan dras är att samtidigt som den generella digitala mognaden, som krävs för att medborgare ska kunna fatta informerade beslut om datadelning, stärks bör också förtroendekapital hos medborgaren byggas av offentlig förvaltning genom transparens som skapar trovärdighet och förståelse för syftet med att dela data.

I en omfattande brittisk studie[12] föredrog en klar majoritet av respondenter ett alternativ för delning av personliga data som inbegrep en statlig reglering och översyn av de datadrivna systemen, offentliga och privata, som hanterar individdata. Valmöjligheter för kontroll utgick ifrån ett standardalternativ för delning där all datainsamling avstannar tills man har tid eller lust att välja hur och när man ska dela sina data, ett så kallat opt-out alternativ.

2.4 Tekniska lösningar för tillit, insyn och kontroll

På senare tid har nya tekniska lösningar presenterats som försöker hantera frågan om tillit genom att ge individen ökad kontroll över sin data och därmed även ökad insyn i hur data delas, till vem och i vilket syfte. Personal Data Stores (PDS) är en sådan lösning och plattformen Solid, skapat av webbens grundare, Sir Tim Berners-Lee tas upp i avsnitt 4.3.6.

En PDS ska ge individen bättre möjligheter att skydda sina data och sin integritet samtidigt som förutsättningar för handel och intäktsgenerering från personliga data stärks. Tidigare identifierade problem kvarstår dock, nämligen att hanteringen av sina egna data kommer att kräva mycket tid och påträffade problem med olika funktioner kan skapa irritation och stress. Det finns en uttalad oro för att överrumplas av förfrågningar om tillgång till data och även här finns en önskan om att kunna avsäga sig ansvaret genom att outsourca detta till en betrodd mellanhand även om ingen sådan finns i nuläget. Lösningen har heller inte lyckats skapa en ökad grad av trygghet bland tillfrågade individer som upplever att man

[11] Delade meningar, Svenska folkets attityder till digital integritet 2020 deladeMeningar2020_Web_1-9A.pdf (insightintelligence.se) sid 16

[12] Public perceptions of good data management: Findings from a UK-based survey, Hartman, Kennedy, Steedman, & Jones, 2020; Steedman et al., 2020, sid. 8-21

inte har ett juridiskt skydd i fall av tvister eller påkommen icke-godkänd hantering av personliga data. Sammanfattningsvis förespråkar tillfrågade individer en metod som ger individen kontroll över sina data men där lösningen inkluderar en tillhörande reglerande enhet, möjligen statlig, som kan tillhandahålla stöd till individen i själva tillsynen av datahanteringen och i fall av rättsliga tvister med aktörer som ingår i datadelningsekosystemet.

2.5 Det ekonomiska värdet av personuppgiftsmobilitet

EU-kommissionen har i sin strategi för data anfört att stora värden kan nås genom att individen får ökad kontroll över sin data. Överväganden om konsumenternas inflytande ligger delvis till grund för bestämmelserna om tillgång till och vidareutnyttjande av data i betaltjänstdirektivet. I likhet med vad som förespråkas av till exempel MinaData-rörelsen så anser kommissionen att verktyg och metoder som möjliggör för individen att på detaljnivå besluta vad som görs med hens data, kommer att ge betydande fördelar för enskilda, bland annat ekonomiska fördelar.[13]

I en rapport från engelska ministeriet för digitalisering, kultur, media och sport (DCMS) undersöktes 2018 potentialen för att stimulera innovation och konkurrens genom personuppgiftsportabilitet, det vill säga att överföra personuppgifter från en aktör till en annan.[14] Om personliga data från offentlig och privat sektor kan flöda i ett säkert system som ger individer kontroll över sin data, skulle den ekonomiska effekten, i form av ökad produktivitet och konkurrensfördelar, uppgå till cirka £27,8 miljarder vilket skulle motsvara ca 1,5 procent av BNP. Denna uppskattning är behäftad med stora osäkerheter och utgår ifrån ett tidigt skede, det vill säga innan innovation baserad på denna personuppgiftsmobilitet hunnit skapa nya användningsområden.

En tidigare studie fokuserade på att estimera det potentiella marknadsvärdet i Storbritannien för så kallade Personal Information Management Systems eller PIMS.[15] Enligt deras utredning så var organisationer villiga att betala mellan cirka 35 – 60 SEK per relation och för att få behörig åtkomst till individens data och tillåten kommunikation med kunder. Vidare uppskattades det att varje individ i

[13] https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:52020DC0066&from=EN sid 12.

[14] Department of Digital, Culture, Media & Sport (2018) *Data Mobility: The personal data portability growth opportunity for the UK economy*

[15] Ctrl-Shift, *Personal Information Management Systems: An analysis of an emerging market*, 2014.

Storbritannien upprätthåller mellan 30 och 100 relationer med banker, applikationer, återförsäljare, myndigheter och andra organisationer. Genom att kombinera dessa två uppskattningar med antalet vuxna och hushåll i Storbritannien estimerades värdet på PIMS-marknaden kunna uppgå till cirka 135 miljarder SEK i Storbritannien.

3 Erfarenheter från omvärldsanalysen

De viktigaste insikterna och erfarenheterna från de granskade över- och mellanstatliga organisationerna summeras för respektive organisation. Därefter följer en redovisning av de olika länderna där Finland redovisas särskilt. För mer utförlig information och analys hänvisar vi till *Bilaga 2 – Omvärldsanalys* där varje lands genomgång redovisas enskilt.

3.1 EU:s ställningstagande gällande insyn och kontroll

- I EU:s datastrategi fastställs det att det är enhetligt med den allmänna dataskyddsförordningen att ge användarna inflytande över sina egna data och möjlighet att kunna hävda sina rättigheter när det gäller användningen av de data de genererar.
- Möjligheten attribueras till verktyg och metoder som möjliggör att på detaljnivå besluta om vad som görs med uppgifterna. Dessa verktyg beskrivs utan detaljer som personliga dataområden.
- Den juridiska grunden för datadelning mellan privata och offentliga aktörer samt för individens möjlighet till en ökad kontroll över detta dataflöde specificeras inte även om flera kommande utredningar ska förtydliga regler, ansvar och möjligheter.
- Slutmålet för EU är att dra nytta av fördelarna med bättre dataanvändning där data som inkluderar personuppgifter är säkra men ändå kan nyttjas för främjandet av tillväxt och värdeskapande på ett ekologiskt hållbart sätt.
- Standardisering av gränssnitt för dataåtkomst i realtid och att göra maskinläsbara format obligatoriska för data från vissa produkter och tjänster ses som grundförutsättningar.
- EU:s dataskyddsförordning innehåller utökade rättigheter för enskilda, som ska kunna utöva insyn och ha kontroll över sina personuppgifter. Detta innebär även utökade skyldigheter för alla som hanterar personuppgifter.

- Möjliggörare för insyn och kontroll är system för personuppgiftsmobilitet vilket kan skapas utifrån:
  - Krav och standarder för interoperabilitet i enighet med principerna om uppgifternas sökbarhet, tillgänglighet, kompatibilitet och återanvändbarhet (Fair).
  - Single Digital Gateway-förordningen och EU-byggblocken som söker säkerställa att medborgare, företag och förvaltningar drar nytta av sömlösa digitala offentliga tjänster var de än befinner sig i Europa.

3.1.1 EU:s Datastrategi

EU-strategin för data[16] är en strategi för politiska åtgärder och investeringar i dataekonomin under de kommande fem åren. Motiveringen är bland annat att det anses finnas en potential för ekonomisk tillväxt när mer data delas mellan olika sektorer, mellan offentliga aktörer och över nationella gränser inom EU. Strikta dataskyddsregler är etiskt motiverade men kan även fungera som ett verktyg för att säkra allmänhetens tillit till delning av personuppgifter inom EU. Det kan även ses som en avskiljare och potentiell konkurrensfördel gentemot Förenta staterna och Kina som båda anses sakna tillräckliga garantier för enskilda personers integritet.

Det behövs ramverk och infrastruktur som säkrar tillgång till data och som stödjer skapandet av europeiska datapooler vilket möjliggör stordataanalys och maskininlärning. Datastrategin rekommenderar vidare genomförandet av sektoröversyner där rättsliga och andra hinder för användningen av data och databaserade utbud kartläggs. En kommande översyn av den allmänna dataskyddsförordningen anses även kunna resultera i ytterligare åtgärder för att stärka tilliten i europeisk användning av data. Under 2022 kommer EU-kommissionen dessutom ge ut en regelbok för molntjänster vilken kommer utgöra ett kompendium av befintliga uppförandekoder och certifieringar avseende säkerhet, energieffektivitet, tjänstekvalitet, dataskydd och dataportabilitet.

[16] Meddelande från kommissionen till europaparlamentet, rådet, europeiska ekonomiska och sociala kommittén samt regionkommittén, En EU-strategi för data Bryssel 19.2.2020 COM (2020) sid.10

Det är enligt EU:s datastrategi enhetligt med den allmänna dataskyddsförordningen att ge användarna inflytande över sina egna data och möjlighet att kunna hävda sina rättigheter när det gäller användningen av de data de genererar. Strategin belyser att det finns verktyg och metoder som möjliggör att på detaljnivå besluta om vad som görs med uppgifterna. Dessa verktyg beskrivs utan detaljer som *personliga dataområden.*

Enligt datastrategin har dessa verktyg en enorm potential men måste kunna hantera samtycke, applikationer för hantering av personuppgifter (även helt decentraliserade lösningar som bygger på blockkedjeteknik) och kooperativ eller truster för personuppgifter som fungerar som nya neutrala mellanhänder i ekonomin för personuppgifter.[17] Standardisering av gränssnitt för dataåtkomst i realtid och att göra maskinläsbara format obligatoriska för data från vissa produkter och tjänster ses som grundförutsättningar för detta.

Investeringar för utbyggnad av nästa generations infrastruktur för databehandling kommer att samordnas med relevanta myndigheter i medlemsstaterna och med investeringar genom struktur- och investeringsfonderna. Under perioden 2021–2027 finansieras infrastruktur, datadelningsverktyg, arkitektur och styrmekanismer för livskraftiga ekosystem för datadelning och artificiell intelligens.

Med utgångspunkt i pågående arbete med det europeiska öppna forskningsmolnet kommer kommissionen att stödja inrättandet av nio gemensamma europeiska dataområden. Dessa inkluderar gemensamma europeiska dataområden för offentlig förvaltning. Åtgärderna för dataområdet för offentlig förvaltning inriktas på juridiska data och data från offentlig upphandling. Även andra områden av allmänt intresse såsom användning av data för att förbättra brottsbekämpningen inom EU vilket ska utföras i enlighet med EU-rätten, proportionalitetsprincipen och dataskyddsreglerna ingår. Området ses som en möjliggörare för innovativa så kallade govtech, regtech och legaltech tillämpningar.

[17] Meddelande från kommissionen till europaparlamentet, rådet, europeiska ekonomiska och sociala kommittén samt regionkommittén, En EU-strategi för data Bryssel 19.2.2020 COM(2020) sid.11

3.1.1.1 Tillgängliggörande av data

Mer och bättre data behöver tillgängliggöras enligt EU:s datastrategi. Rättslig osäkerhet över vad data kan nyttjas till och av vem hindrar datadelning mellan framförallt företag men är även ett problem för offentlig förvaltning. Förslaget till en förordning om europeisk dataförvaltning[18] som kan komma att hantera vidareutnyttjande av data i allmänhetens intresse och som innehas av privata aktörer, utreds för att även öka delningen av data mellan privata och offentliga aktörer.

Enligt EU:s datastrategi behövs även incitament för att få företag att dela data med varandra i större utsträckning och miljöer för att utvärdera olika möjliga initiativ där offentliga och privata aktörer kan samverka kring möjliga lösningar som skapar värde för individer både i rollen som medborgare och som konsument.[19]

Betydande interoperabilitetsproblem gör det omöjligt att kombinera data från olika källor inom samma sektor eller mellan sektorer och arbete pågår med en förstärkt europeisk interoperabilitetsram för offentliga tjänster som syftar till att insamling och behandling av data från olika källor sker på ett enhetligt och interoperabelt sätt.[20][21]

Även om det tydligt framgår att data från olika källor bör delas i allmänhetens intressen specificeras inte någon juridisk grund för datadelning mellan privata och statliga aktörer som explicit hanterar individens möjlighet till en ökad kontroll över detta dataflöde, för detta krävs ändamålsenlig lagstiftning och tydligare politisk styrning.

3.1.1.2 Personliga dataområden

I datastrategin refereras det till en kommande översyn av den allmänna dataskyddsförordningen som anses kunna resultera i ytterligare åtgärder för att stärka tilliten i europeisk användning av data. Individer kan ges inflytande över sina data genom verktyg och metoder för att på detaljnivå besluta om vad som görs med uppgifterna via vad EU-kommissionen kallar personliga dataområden. Enskilda personers rätt till dataportabilitet stöds av artikel 20 i den allmänna

[18] https://data.riksdagen.se/fil/531EF079-826E-49A7-B9EE-05CC816CB8B0
[19] https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:52020DC0066&from=EN sid. 8
[20] https://ec.europa.eu/digital-single-market/en/news/rolling-plan-ict-standardisation.
[21] https://ec.europa.eu/isa2/eif_en.

dataskyddsförordningen och skulle ge individen mer kontroll över vem som kan få åtkomst till och använda maskingenererade data. Denna utveckling förespås kunna ge betydande fördelar för enskilda personer såsom bättre personliga finanser, minskad miljöpåverkan, underlättad tillgång till offentliga och privata tjänster, bättre hälsotillstånd med mera. Standardisering av gränssnitt för dataåtkomst i realtid och att göra maskinläsbara format obligatoriska för data från vissa produkter och tjänster kan ses som grundförutsättningar för detta.

Enligt datastrategin måste verktygen kunna hantera samtycke, applikationer för hantering av personuppgifter och skapa möjlighet för aktörer att fungera som nya neutrala mellanhänder i ekonomin för personuppgifter. EU-kommissionen anser att sådana verktyg har en betydande potential och behöver en stödjande miljö.

3.1.2 European Blockchain Partnership (EBP)

EU bedriver sedan 2018 ett utforskande utvecklingsarbete kring självägande identitet- (SSI) och blockkedjebaserade lösningar genom initiativet EBP där 29 länder deltar.[22] Via EBP utvecklas infrastrukturen EBSI (European Blockchain Services Infrastructure) med visionen om att nyttja blockkedjor för gränsöverskridande digitala tjänster i europeisk offentlig förvaltning.

Inom ramen för EBSI bedrivs arbetet kring ESSIF (European Self Sovereign identity framework) som bland annat fokuserar på gränsöverskridande informationsutbyte via SSI via specifika standarder. Arbetet anses öka i betydelse allt eftersom fler användningsområden för dessa tekniska lösningar utforskas och då speciellt med hänsyn till möjliggörandet av ökad insyn och kontroll för individen över sina personliga data.

3.1.3 Single Digital Gateway, eIDAS och byggblock

Det är viktigt att utvecklingen av nationella system för delning av personliga data och nyttjandes av redan insamlade data har Single Digital Gateway-förordningen (SDG) i åtanke för att EU ska kunna räkna hem den fulla potentialen för den inre marknaden. SDG innebär tillhandahållandet av 20 gränsöverskridande e-förvaltningstjänster som kräver att den offentliga förvaltningen återanvänder data som medborgare och företag redan har tillhandahållit (the Once Only Principle

[22] https://digital-strategy.ec.europa.eu/en/news/european-countries-join-blockchain-partnership

(OOP)). För att uppnå detta krävs standardisering av datamängder, semantik och en infrastruktur för gränsöverskridande datautbyte.

Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden (eIDAS) är en förutsättning för att SDG-förordningen och datautbytet (OOP) ska kunna fungera på ett tillfredsställande sätt och för att tillitsnivån till erbjudna tjänster kan stärkas.

För att stödja den digitala inre marknaden finansierar Connecting Europe Facility (CEF)-programmet en uppsättning generiska och återanvändbara digitala infrastrukturer (DSI), även kända som EU-gemensamma byggblock.[23] Dessa är även de av potentiell vikt för att bygga tjänster för ökad insyn och kontroll för personliga data. Byggblocken erbjuder grundläggande funktioner som kan återanvändas i alla europeiska projekt för att underlätta leverans av digitala offentliga tjänster över gränser och sektorer.[24] Målet med byggblocken är att säkerställa interoperabilitet mellan IT-system så att medborgare, företag och förvaltningar kan dra nytta av sömlösa digitala offentliga tjänster var de än befinner sig i Europa.

3.1.4 Rättsliga förtydliganden behövs

Under våren 2021 arbetar EU-kommissionen med en genomförandeakt för det tekniska systemet (OOTS - Once-Only Technical System) för en uppgift en gång (OOP – Once Only Principle)) inom SDG-förordningen.[25] Medlemsstaterna får utkast för att kunna komma med synpunkter och senare via ett kommittéförfarande rösta om förslaget. Senast den 12 juni 2021 ska EU-kommissionen anta genomförandeakten med dess tekniska och operativa specifikationer för det tekniska systemet som behövs för genomförandet av Artikel 14 (9) i SDG-förordningen. I ett expertutlåtande avseende det första utkastet till SDG-förordningens genomförandeförordning för det tekniska systemet för OOP[26] anger DIGG att man i dagsläget inte anser att det är tillräckligt tydligt om

[23] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/What+is+a+Building+Block

[24] Se avsnitt 4.1 och 4.2 för mer om Sveriges utveckling av en förvaltningsgemensam digital infrastruktur och byggblock

[25] Begreppet OOP användas ibland mer fristående från SDG-förordningen för att t.ex. beskriva nationella lösningar för En-uppgift-en-gång, exempelvis Estlands nationella lösningar som baseras på deras X-Road-infrastruktur istället för CEF-byggblocket eDelivery som krävs för att uppfylla informationsutbytet för OOP enligt SDG-förordningen

[26] PM – expertutlåtande avseende SDG-förordningens genomförandeförordning för ett tekniskt system för gränsöverskridande automatiskt utbyte av bevis och tillämpning av engångsprincipen

den rättsliga grunden kommer att baseras på överföring mellan myndigheter eller via användaren. Den föreslagna arkitekturbeskrivningen och de tekniska specifikationerna över hur det tekniska systemet ska fungera innehåller för stor osäkerhet och enligt utlåtandet anser DIGG att nuvarande förslag på genomförandeförordning för OOP inte uppfyller kraven i Artikel 14 (9) i SDG-förordningen.

Kommissionen anser i en konsekvensbedömning[27] att användaren, genom mekanismen med *förhandsgranskning av bevis* bibehåller sin användarkontroll och detta kan tolkas som om beviset går via användaren medan tidigare bedömningar angett att det rör sig om ett utbyte mellan myndigheter. Utifrån svensk rätt borde svaret på denna fråga bli centralt för att avgöra behovet av författningsåtgärder gällande till exempel svensk sekretesslagstiftning och registerförfattningar.

Utvecklingsarbetet inom EU och uppdrag i författningen att utforma myndighetssamverkande kontaktpunkter och andra gemensamma funktioner för myndigheter och företag har fört med sig ett antal juridiska utmaningar. I eSams rapport *Eget utrymme hos en myndighet – en vidareutveckling*[28] tas det upp att det egna utrymmet utvecklas som koncept. När olika myndigheter kan nås via samma ingångssida och ett eget utrymme kan erbjudas av flera myndigheter, så som exempelvis inom verksamt.se, utvecklas ett så kallat *gemensamt eget utrymme*.

Tanken är att innehavaren av utrymmet ska vara en och samma myndighet medan flera myndigheter ska anses tillhandahålla utrymmet. Det gemensamma egna utrymmet är en portaltjänst där besökaren får legitimera sig och väl inne i det gemensamma egna utrymmet ser användaren inte olika lokaler utan bara ett enda myndighetsgemensamt utrymme.

Drift och förvaltning av gemensamma egna utrymmen måste förenas med gällande rätt och enligt rapporten blir ett antal frågor aktuella att besvara som berör vem som ansvarar för vad inom utrymmet. Till detta kommer frågor om vilken myndighet som ska pröva en begäran om en allmän handling eller

[27] Konsekvensbedömning (DPIA - Data Protection Impact Assessment) är inte ett slutligt utlåtande från europeiska datatillsynsmannen (EDPS). Utlåtande från EDPS som är avgörande för genomförandeförordningen för OOP förväntas komma 12 maj 2021.

[28] https://www.esamverka.se/download/18.4472a99d1784abb64fe55a6e/1617090755211/V%C3%A4gledning%20eget%20utrymme%20hos%20myndighet%20210312.pdf

sekretesspröva information som finns i utrymmet eller stå ansvarig enligt den författningsreglering som gäller för ärendehandläggning, dataskydd och informationssäkerhet. Gemensamma utrymmen kan skapa oklarheter i fråga om ansvaret mellan myndigheter men även mellan myndigheter och den individ som använder utrymmet som måste veta vart hen ska vända sig när denne vill utöva sina rättigheter enligt gällande rätt. eSam poängterar att långsiktig hållbarhet främjas av att varje myndighet själv har den juridiska rådigheten över sina informationstillgångar och ensam ansvarar för funktioner som myndigheten tillhandahåller åt andra.

3.2 Förenta Nationernas (FN) ställningstagande kring digital identitet

I granskningen av FN:s olika skrivelser gällande insyn och kontroll så som begreppen definierats i detta uppdrag, så har relevanta utlåtanden mest handlat om ställningstaganden kring digitala identiteter. I fokus står möjligheten att använda någon form av universell digital identifiering för att kunna säkerställa en individs identitet. Detta skulle vara ett exempel på att ge ökad kontroll till individen över data om individens identitet. I förlängningen skulle det kunna innebära att fler individer skulle kunna få tillgång till egna utrymmen för data om individen, hens livssituation och ärenden med myndigheter och organisationer.

- 2018 skapades ett manifest med stöd från FN:s flyktingkommission (UNHCR) där förmågan att kunna bevisa sin identitet likställs med en grundläggande och universell mänsklig rättighet.
- I en digital kontext innebär ovan att ett globalt e-ID system bör utvecklas vilket kan ha konsekvenser för hur vi lagrar information om vår person och vem som har tillgång till denna information och hur tillgång ges.
- Endast 3 procent av utvecklingsländerna har grundläggande ID-scheman där eID kan nyttjas för mer än identifiering. Det finns dock inga klara mätningar på användares nöjdhet med olika lösningar eller vad som utgör en eID-lösning som ger ökad insyn och kontroll över användarens personliga data.

3.2.1 ID som mänsklig rättighet

Nyligen antog FN en *mänsklig rättighetsbaserad strategi för data* som kallas HRBAD (A Human Rights Based Approach to Data). Strategin fokuserar på frågor om datainsamling och ska syfta till att sammanföra relevanta dataintressenter och utveckla praxis som förbättrar kvaliteten, relevansen och användningen av data och statistik i överensstämmelse med internationella normer och principer för mänskliga rättigheter.[29] Strategin är en del av arbetet med mål 16.9 av de globala hållbarhetsmålen som handlar om att säkerställa juridiska identiteter för alla senast 2030 inklusive födelseregistrering.[30]

Kopplingen till kontroll över personliga data kommer genom vissa av de preliminära principer och rekommendationer som formulerats av HRBAD såsom uppdelning av data (data disaggregation). Individer borde kunna välja fritt om de vill dela information eftersom detaljerade personliga data, i synnerhet insamlad från marginaliserade grupper, kan användas i ont uppsåt. HRBAD anser att individers självuppfattade grupptillhörighet borde utgöra grunden för kategorisering av individer i populationsgrupper. För detta krävs nya verktyg och digitala infrastrukturer som inte preciseras men som det inletts vissa sammankomster och workshops kring.

3.2.1.1 ID2020 – Ett digitalt universal ID

År 2020 organiserades ID2020 av FN där privata företag såsom Microsoft och Accenture samlades tillsammans med humanitära grupper inklusive World Food Programme och FN:s flyktingbyrå. Det gemensamma målet var att skapa digitala identiteter för alla människor, kopplad till fingeravtryck, födelsedatum, hälsojournaler, utbildning, resor, bankkonton och mera.[31] Fokus låg primärt på att visa på möjliga framtida lösningar än att bygga konsensus kring en specifik lösning. Accenture demonstrerade till exempel en prototyp i form av en app som bland annat använder QR-koder för att identifiera individer.[32] Farhågor om att samla så mycket information om en individ på en plats anses kunna komma att hanteras med lösningar baserade på blockkedjeteknologi.

[29] https://www.ohchr.org/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf
[30] Mål 16: Fredliga och inkluderande samhällen - Globala målen (globalamalen.se)
[31] https://id2020.org/digital-identity
[32] https://youtu.be/QYy8a7HDJ0g

2018 skapades ID2020-alliansens manifest[33] i samarbete med FN:s flyktingkommissarie (UNHCR) med etiska överväganden kring digital identitet. Där likställs förmågan att kunna bevisa sin identitet med en grundläggande och universell mänsklig rättighet och att komplement till traditionella nationella identitetshandlingar borde utvecklas utanför styrande regimers kontroll. Individer borde ha kontroll över sina egna digitala identiteter och över hur data kring deras identitet samlas in, används och delas, men för att decentraliserade digitala identiteter ska erkännas och vara betrodda behövs först konsensus om styrande principer, designmönster, interoperabilitetsstandarder och andra policyramverk.

3.2.2 eID och mätningar på utveckling

I dagsläget är de flesta digitala ID-system kopplade till specifika funktioner och tjänar en delmängd av befolkningen och många nyttjas enbart för identifiering. Enligt världsbanken har endast 3 procent av utvecklingsländerna grundläggande ID-scheman som kan användas för att komma åt en rad online- och offline-tjänster.[34] 24 procent hade inget digitalt ID-system över huvud taget.

Att det inte finns etablerade verktyg för att mäta medborgares tillfredsställelse med tjänster inom e-förvaltning utgör ett problem för benchmarking av prestandaförbättringar. Initiativ som försökt utveckla en medborgarnöjdhetsmodell har saknat ett systematiskt tillvägagångssätt[35]. Det som kommer närmast en utvärdering av offentliga e-tjänster är eGovernments Benchmark-rapporten som utgår ifrån principer satta i eGovernment Action Plan 2016-2020 och Tallinn Deklarationen. Här nyttjas åtta livshändelser som utvärderas vartannat år. Sverige anses ligga i den högsta kategorin av länder i termer av digitala offentliga tjänster med människocentrerad design och digital mognad inom offentlig förvaltning även om det finns förbättringsområden såsom inom öppenhet det vill säga publicering av öppna data.

eID är en indikator i sig som bedöms utifrån om det finns ett e-ID system och om det går att nyttja i andra länder. Det finns ingen skala som bedömmer e-ID-lösningen i sig eller medborgares nöjdhet med nationella lösningar.[36] Det är

[33] https://id2020.org/manifesto
[34] World Development Report 2016 s. 194-195,
[35] https://cordis.europa.eu/article/id/88500-optimising-egovernment-services-for-citizens
[36] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62368

därmed svårt att veta vad som utgör postiv utveckling inom e-ID utöver dessa faktorer.

3.3 OECD:s fokus på policy kring insyn och kontroll

3.3.1 OECD Digital Government Index (DGI) 2019[37]

- OECD:s Digital Government Index uppmanar generellt sätt länder till tydligare styrning, kompetensutveckling inom offentlig sektor och samproduktion med användare.
  - Ett av målen är ökad proaktiv styrning men nämner inte möjligheten för den enskilde att styra över sin datas användning och delning som en del av denna policy.
  - I utvärderingen av dimensionen *datadriven offentlig sektor* anses Sverige vara lågpresterande och ett tydligt bristområde är publicerad öppna data. Det framgår dock inte att en öppen och transparent offentlig sektor betyder ökad insyn i personliga data såsom detta definieras inom detta uppdrag.

Utvärderingen baseras på hur olika länder presterat utifrån olika dimensioner som en helt digital offentlig förvaltning bör uppvisa. Storbritannien, Japan och Danmark pekas ut som exempel på länder som lyckats bäst genom ett helhetstänk i deras respektive digitaliseringsstrategier. Indexet består av återkommande förslag om bättre och tydligare styrning, vikten av rätt kompetens inom offentlig förvaltning och fördelar med att inkludera användarna av digitala tjänster i designprocesser.

Det finns inget som direkt kopplar till frågan om individens ökade insyn och kontroll över personliga data och hur detta skulle påverka ett lands ranking i DGI. Dimensionen *en öppen och transparent offentlig sektor* lyfter inte ökad insyn i personliga data såsom det definieras inom detta uppdrag som en faktor utan fokus är på publicerade öppna data och krav på standarder och interoperabilitet som detta kräver.

I utvärderingen av dimensionen *datadriven offentlig sektor* påverkas resultatet av huruvida medborgare och företag har tillgång till, möjlighet att ge samtycke för och

[37] OECD Digital Government Index (DGI): 2019 - OECD

rätten att vägra, datadelning med offentlig sektor och tredje part.[38] Hur man lyckats med detta utifrån hur man hanterat faktiska och upplevda legala hinder utifrån GDPR, nationell lagstiftning eller praxis analyseras inte. Det finns heller ingen jämförelse av förvaltningsmodeller och vilka förutsättningar dessa ger för att uppnå önskade resultat på ett specifikt sätt som värdesätts av detta index. På sätt och vis belönas nationella strategier som söker centralisera hantering, förvaring och delning av data och som ger breda mandat till en nationell samordnare att styra förvaltningsgemensam digitaliseringspolicy.

Lågpresterande länder på denna dimension såsom Tyskland, Chile och Sverige måste enligt rekommendationerna anta en helhetsstrategisk strategi för tillgång till och delning av data, med särskild tonvikt på att utnyttja infrastruktur, standarder och metoder för datadelning som gör det möjligt för organisationer inom den offentliga sektorn att göra effektiv och strategisk användning av data.[39]

3.4 Erfarenheter från Norden och övriga länder

Följande sju länder har analyserats; Finland, Norge, Danmark, Frankrike, Storbritannien, USA och Indien.

Myndigheterna i de nordiska länderna har en lång tradition av att samla in data om individen, men det finns utmaningar för myndigheter att utveckla sina förvaltningsstrategier i ett digitalt ekosystem där innovation och dataekonomi är ledord. Sverige, Finland och Norge har haft ambitiösa mål att bli världsledande i utvecklingen av e-förvaltning och särskilt Danmarks omstrukturering av sin offentliga administration har uppmärksammats för att tidigt sökt inkorporera EU:s uppmuntran till hållbar utveckling.

De nordiska ländernas dataregister är inte bara unika för att de funnits så länge, de är också unika för att de har ett juridiskt mandat som ger olika myndigheter tillåtelse att samla in och underhålla uppgifter om befolkningen. Medborgarna saknar ett opt-out alternativ eftersom systemen utgör en central del av hur själva välfärdssystemet fungerar. För att systemet ska fortsätta fungera i takt med medborgares ökade förväntningar på offentlig service så riskerar man att anta att alla bemyndiga medborgare förstår konsekvenser, kostnader, nyttor och risker

[38] Digital Government Index: 2019 results Sid. 20 4de9f5bb-en.pdf (oecd-ilibrary.org)
[39] Digital Government Index: 2019 results Sid. 30 4de9f5bb-en.pdf (oecd-ilibrary.org)

med att dela personliga data (eller att inte göra det). Utan detta antagande problematiseras grunden på vilken mer och mer insamlade data förväntas nyttjas för effektivare offentliga tjänster byggda på datadelning med samtycke som grund.

Hur balansen mellan effektivitet, rättssäkerhet, medborgarfokus och harmonisering med överstatliga initiativ säkras, skiljer inte bara de nordiska länderna åt utan är särskiljande för alla länder när de kombineras med andra förutsättningar såsom landets digitala mognad och samt vilken styrningsmodell som råder och om det är ett land med relativt stor eller liten befolkning.

Nedan återges aspekter av Finlands angreppsätt gällande att ge medborgare ökad insyn och kontroll över personliga data innan en summering ges från omvärldsbevakningen i sin helhet. För centrala erfarenheter från varje enskilt land hänvisar vi till *Bilaga 2 Omvärldsbevakning*.

3.4.1 Finland

- Uttalad hög ambitionsnivå gällande att ge individen insyn och kontroll över personliga data och att ge staten möjlighet att nyttja denna data för att skapa en proaktiv offentlig sektor med insyn i individers möjliga framtida behov av offentliga tjänster.
- Insyn via till exempel portaler som samlar information och tillhandahåller egna sidor är en väl etablerad policy men det finns begränsningar i kontrollen individen har över sina data, till exempel kan man inte välja att inte dela data för forskning.
- Lagen om sekundär användning av hälso- och sociala data från 2019 anses av vissa som kontroversiell då kritiker anser att den inte föregåtts av öppen debatt och de varnar för icke-kompatibilitet med GDPR samt användning av insamlade data för andra syften än den samlats in för. Särskilt avsnitt 24 som ger undantag för administrativa böter om brott mot GDPR inträffar ses som problematisk.

Finland omnämns ofta som föregångsland inom området dataportabilitet, inte minst för att MinaData-principerna som har fått internationell spridning och omnämns i EU:s datastrategi, har sitt ursprung i finska The Open Knowledge Festival och att MyData Global har sitt huvudkontor i Finland. Finland har utmärkt sig bland annat genom att koppla ihop offentliga tjänster (till exempel

Aurora-nätverket, en AI-baserad virtuell assistent som guidar medborgare till offentliga tjänster utifrån deras användardata och livssituation) eller genom att samla information på ett ställe (se soumi.fi nedan). Detta ger medborgare en upplevelse av mer sömlösa flöden mellan olika myndigheter i utförandet av ett ärende. Målet är att i allt högre grad möjliggöra proaktivt agerande från myndigheter i enskildas ärenden i syfte att skapa välstånd för individen och samhället i stort. Till exempel genom att nyttja olika datakällor för att skapa en individualiserad hälsoprofil.

Suomi.fi är en nättjänst som samlar ihop tjänster och anvisningar för medborgare, och företag utifrån livshändelser. Individer kan via sidan ge och begära fullmakter (elektroniska befullmäktigandes uppgifter sparas i fullmaktsregistret) och kontrollera sina registeruppgifter. På Suomi.fi-registren kan individen se de uppgifter som finns i vissa myndigheters register. Varje registerförare väljer vilka uppgifter som visas och anvisningar finns i anslutning till varje register för hur individen kan rätta eller begära rättelse av felaktiga uppgifter.

Ett exempel på framgång med e-förvaltning är att 50 procent av befolkningen mellan 18–65 år och 37 procent av personerna över 65 år använt Mina Kanta-sidor[40] där medborgare kan se egna hälsouppgifter och recept. Patienter kan även ge eller återkalla samtycke till vilka andra som kan se patientens hälsoinformation. Egengenererade data från godkända hälsoapplikationer kan sparas i datalagret för egna uppgifter på Mina Kanta-sidorna och inkluderar i nuläget vikt, steg och daglig aktivitet. All användning av Kanta-tjänsterna registreras i en logg vilket ger insyn i vilka hälso- och sjukvårdsorganisationer som behandlat ens uppgifter. Patienter har dock inte möjlighet att kontrollera om deras hälsouppgifter får användas för forskning.

Den finska visionen pekar mot att all information och data kan och bör göras tillgänglig via en enda plattform, där åtkomst och anslutning till olika plattformar blir så sömlös och smidig som möjligt för användaren. I regeringens framtidsrapport från 2018[41] likställs digitaliseringen med möjligheten att skapa en offentlig sektor som agerar proaktiv till exempel med åtgärder för individers

[40] https://www.kanta.fi/sv/web/guest/blogg/-/asset_publisher/1QjC602jKPR6/content/omakannan-kavijamaarat-selvassa-kasvussa

[41] Government Report on the Future, Part 2, Solutions to the transformation of work sid. 42

hälsoutveckling. För detta krävs dock tillgång till, och ett kombinerande av data från flera olika källor om individen.

Finland har satsat på en övergripande ekosystemlösning med systemintegration för att göra data mer tillgänglig[42] men det finns juridiska frågetecken kring sekundär användning av data. Rättigheten till ett informerat självbestämmande och till sina personliga data enligt MinaData-principerna, har inte säkrats eller varit föremål för öppen allmän debatt. Istället har man valt att inkludera ett undantag för eventuella kränkningar av GDPR i landets egna dataskyddslag.[43] Ambitionsnivån och angreppsätt har resulterat i att vissa kritiska röster höjts kring kompatibilitet av visionen med till exempel GDPR och invånarnas framtida förmåga till självbestämmande.

3.4.2 Summering av medtag från omvärldsbevakningen

Det är vanligt förekommande för de länder som finns med i omvärldsbevakningen att utgå ifrån livshändelser när individers insyn och kontroll över personliga data ska ökas men i vissa fall är det helt enkelt de aktörer som är villiga att ingå i testmiljöer som avgör lösningars utformningar och fokusområden.

Tekniska lösningar, ekonomiska medel och tydlig politisk styrning varierar mellan de länder som granskats men omnämns sällan som ett hinder för utveckling av ett koncepttest eller lösning. Det är oftast juridiska tolkningar och osäkerhet som framstår som mest problematiskt och ett hinder för utveckling på området. Det finns även oklarheter i alla länder över vilka incitament och förutsättningar (utöver juridisk säkerhet) som skulle motivera individer och näringsliv att mer aktivt efterfråga ökad insyn och kontroll för den enskilde medborgaren.

Inom projekt- eller testmiljöer läggs fokus på samskapande mellan privata och offentliga aktörer där delar av en modell för delning av personliga data kan utvärderas utifrån funktionalitets- och värdeskapandeperspektiv för individen. Privata aktörer kan delta utan att först behöva göra stora investeringar eller utvärdera nya affärsmodeller. Delar av lösningar kan ses i alla länder men inget land har inkorporerat ett holistiskt ekosystem för delning av personliga data

[42] Aula, V. 2019. Institutions, infrastructures, and data friction–Reforming secondary use of health data in Finland. Big Data & Society, 6(2), 2053951719875980

[43] Big Data & Society January–June: 1–13, Aaro Tupasela, Karoliina Snell, Heta Tarkkala1 2020 DOI: 10.1177/2053951720907107

mellan individ, offentlig aktör och privat aktör där både insyn och kontroll över personliga data styrs av individen själv.

Det finns exempel på nerifrån-upp initiativ, ofta inspirerade av Finlands MinaData organisation och dess principer, där start-ups och innovativa intresseföreningar skapar olika pilotprojekt i testmiljöer och inom regulatoriska sandlådor. Det finns även exempel på projekt med regeringen som initiativtagare och där politisk vilja i kombination med en möjlighet och vilja att finansiera projekt, skapar engagemang från flera olika aktörer. I de flesta fall ses offentlig sektors involvering som nödvändig utifrån privatpersoners involvering i dessa projekt, för att skapa tillit till datadelningssystem och säkerheten i den nödvändiga digitala infrastrukturen. I båda fallen finns det behov av arenor för offentliga och privata aktörer att samproducera lösningar utifrån tydligt identifierade medborgarbehov. Det kan handla om en del av en livshändelse eller ett exempel på en affärsmöjlighet som ett företag vill utforska. Såväl offentliga aktörer som medborgare och näringsliv behöver dock en gemensam förståelse för vad dataportabilitet innebär och hur befintliga strukturer, affärsmodeller och policy påverkas av att ge individen ökad insyn och kontroll av såväl personliga data som hålls av offentlig förvaltning som av konsument- och beteendedata som hålls av företag och organisationer. Omställningen är komplex och behovet av testmiljöer samt expertis i att designa digitala miljöer kan anses högt.

Det behöver skapas tydliga incitament för alla parter i värdekedjan att nyttja delade data, från individen till organisationer. Individer behöver inse hur data kan nyttjas och vad det kan innebära för nytta för dem, exempelvis nya värdeskapande tjänster, annars kommer lösningar för ökad insyn och kontroll endast leda till inaktivitet och en minskning av delade data. Detta ställer höga krav på designen och gränssnitt som påverkar användarupplevelse och generering av engagemang i fortsatt användning av de tjänster som leverantörer av olika utrymmen för insyn och kontroll erbjuder.

Företag behöver se nya möjligheter och affärsmodeller med att deras kunder kontrollerar mer av interaktionen dem emellan. Annars kommer de inte ingå i initiativ som söker utforska möjligheterna till ökad innovation och värde-skapande. Det finns även en tydlig koppling mellan näringslivets intresse i att utforska nya möjligheter och möjligheten att finansiera deltagandet i ett experiment eller statligt initiativ genom finanser öronmärkta för projekt inom företagets sociala ansvarsstrategi. Det vill säga att i de fall där det inte finns ett

tydligt vinstintresse för att engagera företag så kan det finnas ett intresse att delta utifrån att deltagandet kan skapa välvilja bland allmänheten och bidra positivt till varumärkesutvecklingen av ett visst företag eller organisation.

4 Nationella förutsättningar och initiativ

4.1 En förvaltningsgemensam digital infrastruktur är under utveckling

Regeringen uppdrog åt nio myndigheter att tillsammans etablera en förvaltningsgemensam digital infrastruktur som ska möjliggöra ett effektivt och säkert utbyte av information inom och med det offentliga.[44] Syftet med uppdraget är att stärka det offentligas förmåga att leverera effektiv, säker och innovativ digital service till invånare och företag. Regeringen har också gett i uppdrag till DIGG att analysera förutsättningarna för kommuner och regioner att delta i den förvaltningsgemensamma digitala infrastrukturen för informationsutbyte.[45]

Den förvaltningsgemensamma digitala infrastrukturen består i sin enklaste form av ett antal byggblock som tillsammans utgörs av en mängd olika standarder, ramverk, modeller, strukturer och tjänster. Vart och ett av byggblocken skapar nytta genom att skapa förutsättningar för annan digital utveckling. Byggblocken delas in i fyra olika kategorier: *Digitala tjänster, Informationsutbyte, Informationshantering* och *Tillit och säkerhet.*[46]

Infrastrukturens utveckling och förvaltning behöver struktur för styrning och den infrastrukturansvarig leder det strategiska arbetet i samråd och samverkan med andra aktörer. I delredovisningen av regeringsuppdraget föreslår vi att DIGG ska ha rollen som övergripande ansvarig för infrastrukturen (infrastrukturansvarig).

4.2 Den förvaltningsgemensamma digitala infrastrukturen består av byggblock

I detta avsnitt redogörs för några av de byggblock som bedöms kunna skapa förutsättningar för en ökad insyn och kontroll över de data om individen som finns hos offentlig sektor, och i förlängningen hos privat sektor. Som nämnts ovan

[44] Regeringen (2019) *Uppdrag att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte* Dnr I2019/03306/DF

[45] Regeringen (2020) *Uppdrag att genomföra en analys om förutsättningar för kommuners och regioners deltagande i den förvaltningsgemensamma digitala infrastrukturen* Dnr I2020/02241/DF

[46] DIGG m.fl. (2021) *Uppdrag att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte*

och som även framgår av den delrapport som lämnats i januari[47] och de byggblocksbeskrivningar[48] som är publicerade, är byggblocken indelade i fyra kategorier.

4.2.1 Digitala tjänster

Med digitala tjänster avse byggblock som är förutsättningsskapande för att effektivare kunna utveckla användarnära kundmöten. Exempel på digitala tjänster är Mina ombud, Mina ärenden, Min profil och digital post.

4.2.2 Informationsutbyte

Med informationsutbyte avses byggblock som skapar standardiserade mönster eller gemensamma infrastrukturtjänster för utbyte av information. Inom kategorin finns byggblocken Adressregister, API-hantering och Meddelandehantering.

4.2.3 Informationshantering

Med informationshantering avses byggblock som medför möjlighet till standardiserad maskinläsbar tolkning av egenskaper hos information och informationstjänster. Inom kategorin finns byggblocken Indexering och Metadatahantering.

4.2.4 Tillit och säkerhet

Byggblock inom kategorien tillit och säkerhet bidrar till att möta behoven av säkerhet. Inom kategorin finns byggblocken Auktorisation, Identitet, Spårbarhet, Tillgänglighet och Tillitsramverk.

4.3 Individcentrerade dataekosystem

Ekosystem och plattformar är etablerade termer både inom privat och offentlig sektor. De används för att beskriva samverkan och användandet av gemensamma resurser och de beroenden som uppstår i ekosystemet eller på plattformen.

4.3.1 Generellt om digitala ekosystem

För att offentlig förvaltning och företag ska lyckas med att utveckla mer sammanhållna, individcentrerade och sömlösa tjänster utifrån livshändelser finns ett stort behov av att anlägga ett helhetsperspektiv. Det innebär att tekniska,

[47] DIGG m.fl. (2021) *Uppdrag att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte*

[48] https://www.digg.se/utveckling-av-digital-forvaltning/digital-infrastruktur/samverkansaktor#rapporter_och_redovisningar

rättsliga, semantiska och organisatoriska förutsättningarna behöver ses som en helhet, ett ekosystem.

Ett digitalt ekosystem är en avgränsad teknisk miljö bestående av infrastruktur, digital utrustning, digitala resurser (tjänster, applikationer och programvara) och användare som samverkar med varandra. De digitala ekosystemen har många gånger anammat principer från naturens ekosystem. I de digitala ekosystemen kan aktörerna samspela för att generera ett värde för sina användare/kunder, sig själva och i förlängningen även varandra.

Till skillnad från biologiska ekosystem finns det i digitala ekosystem ofta en huvudaktör som initierat ekosystemet där övriga aktörer i ekosystemet kan använda infrastrukturen för att skapa värde. Huvudaktören benämns på olika sätt beroende på ansvar, typ av ekosystem etc. men vanligt är att det framgår att aktören är ansvarig för ekosystemet.

De digitala ekosystemen avgränsas ofta mot sin omvärld genom överenskomna regler för hur systemen i ekosystemen ska fungera ihop och kommunicera med varandra. Denna interoperabilitet kan ske organiskt och decentraliserat (jmf hur internet är uppbyggt) eller toppstyras av en aktör.

Ofta finns det en marknad knuten till de digitala ekosystemen där plattformsledaren respektive tredjepartsutvecklarna kommer överens och kan erbjuda sina respektive produkter och tjänster i kombination eller var för sig.

4.3.2 Olika typer av digitala ekosystem

Affärsekosystem består av nätverk av olika aktörer såsom företag, forskningsinstitut samt offentliga aktörer som samarbetar över sektorsgränser för att skapa nya produkter och tjänster. AppStore och PlayStore är två exempel på affärsekosystem där tredjepartsutvecklare erbjuder sina appar som bygger på de underliggande plattformarna iOS respektive Android. Plattformsledarna, Apple respektive Google, sätter spelreglerna för till exempel vilka som får sälja och distribuera sina applikationer, vilka krav som måste uppfyllas samt vilken provision som ska betalas tillbaka från en genomförd transaktion.

I ett *dataekosystem* läggs istället fokus direkt på den data som delas och hur den flödar mellan aktörerna inom ekosystemet.[49] Ofta finns det en plattform, en infrastruktur, där data delas med hjälp av API:er.[50] Aktörerna kan utgöras av både individer och organisationer. Ett exempel på ett dataekosystem är DIGG:s dataportal för öppna data. Målet med portalen är att öka Sveriges förmåga att tillvarata data som strategisk resurs och förbättra digital samverkan mellan det offentliga, näringslivet och civilsamhället.[51]

4.3.3 Styrningen och ägandet av dataekosystem

Digitala ekosystem styrs genom fördelning av rättigheter och ansvar bland ekosystemets aktörer samt genom nödvändiga regler och processer.[52] Styrningsstrukturen fastställs vanligtvis av den aktör som antar rollen som plattformsledare som därmed beslutar om och underhåller plattformen. Den ansvarige har ofta ett övergripande ansvar för infrastrukturen och för att säkerställa att endast aktörer och tjänster som uppfyller vissa villkor ansluts samt att de efterlever uppsatta krav och åtaganden.

Utöver plattformsledaren kan ekosystemet på olika sätt påverkas av andra aktörer. Det kan dels vara ägarna själva, formella eller informella partners, producenter till betydelsefulla datamängder, organisationer med stora användarbaser samt organisationer och individer med ett aktivt engagemang i ekosystemet. Därutöver behöver ett ekosystem förhålla sig till gällande rätt, det vill säga de rättsregler som är tillämpliga där ekosystemet ska verka. Det handlar bland annat om EU:s dataskyddsförordning och eventuellt tillhörande nationell reglering om ekosystemet ska behandla personuppgifter.

Ekosystemets plattform kan ha en eller flera ägare och i olika konstellationer.

Ensamt offentlig ägande innebär att en offentlig aktör, ofta en myndighet, ensamt äger eller utgör plattformsledaren. Ett exempel på en sådan plattform är Arbetsförmedlingens ekosystem *JobTech Dev* där externa tjänsteleverantörer kan, genom att använda data från Platsbanken, erbjuda digitala tjänster för bättre jobbmatchning till arbetssökande.

---

[49] Lindman et al., 2015
[50] Linåker & Runeson, 2020
[51] https://www.digg.se/om-oss/nyheter/2020/digg-lanserar-sveriges-nya-dataportal
[52] Alves et al., 2017

Offentligt samägande innebär att två eller fler offentliga aktörer äger eller utgör plattformsägare i ett konsortium. Ett exempel på en sådan konstellation är HSL Developer Community som är ett dataekosystem fokuserat på kollektivtrafiken inom Helsingforsregionen i Finland. Plattformsledaren HSL/HRT är ett företag som är samägt av kommunerna inom regionen.

Offentligt–privat samägande är när två eller fler offentliga och privata (eller civilsamhälles-) aktörer äger eller utgör plattformsägare i ett konsortium. Ett exempel utgörs av Trafiklab som är ett dataekosystem för den svenska kollektivtrafiken. Plattformsledaren utgörs av Samtrafiken som är det företag som är samägt av de regionala kollektivtrafikbolagen tillsammans med privata operatörer.

I fallet med ensamt privat ägande kan plattformarna Appstore och Playstore utgöra konkreta exempel.

4.3.4 Exemplet MinaData

MyData Global är en intresseorganisation med målsättning att bland annat stärka individens egenmakt i relation till data om sig själv, stärka individens möjligheter att fatta välgrundade beslut samt samverka mer medvetet och effektivt med organisationer som skapar eller använder individens personliga data. I Sverige används begreppet MinaData för att beskriva MyData.

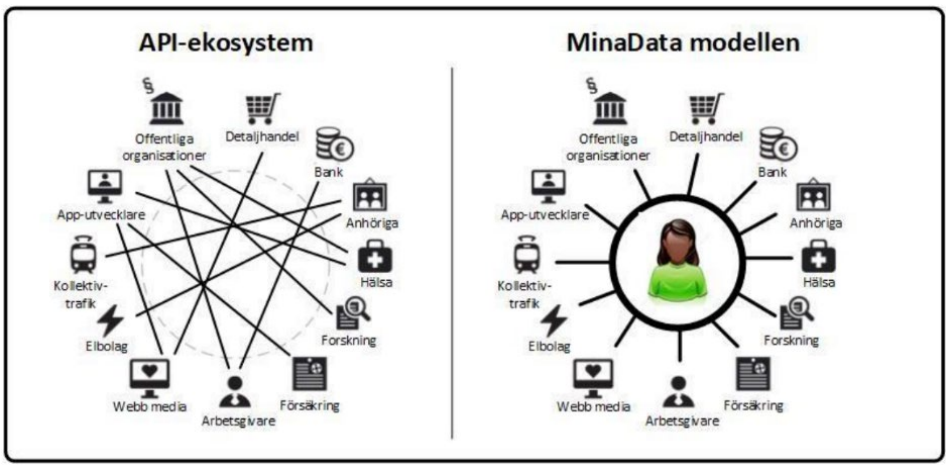
MyData Global har tagit fram följande principer för hur individcentrerade dataekosystem bör utformas:

- Individen ska ha full förståelse över och insyn i policyer, avtal och hur hens data används
- Individen ska ha befogenhet att ge, neka eller återkalla sitt samtycke till delning av data
- Individen i centrum när tjänster behöver data från varandra
- Individen ska säkert kunna hantera sina personuppgifter på det sätt hen föredrar
- Dataportabilitet ska främjas mellan tjänster och lagringsytor
- Interoperabilitet ska främjas så att alla personuppgifter är flytt- och återanvändbara utan att individen förlorar kontrollen.

4.3.5 eSams modell för individcentrerad informationshantering

eSam har i en rapport från 2020 tagit fram en modell för individcentrerad informationshantering som inspirerats av principerna bakom MinaData, bland annat att data om individen är en resurs som individen ska ha tillgång till och kontrollera.[53]

Figur 1 MinaData modellen



eSams modell är framtagen för att komplettera dagens mer API-baserade ekosystem genom att utgå från individens behov av att hantera olika livshändelser och rättigheter kopplade till uppgifter som sig själv. Syftet med eSams modell är att stärka individens roll i det digitala informationsflödet mellan offentliga organisationer samt öka individens kontroll över hur hens personuppgifter hanteras.

En central komponent i eSams modell är ett så kallat ”MinaData-konto” som ska ge individen möjlighet att se relevant data, hur samtycken hanteras och andra viktiga funktioner. Enligt eSam skulle en sådan modell ge individen möjlighet att på ett enkelt sätt godkänna olika dataflöden mellan organisationer.

4.3.6 Exemplet Solid

Solid (Social Linked Data) är ett projekt med syftet att decentralisera webben och ge kontrollen av personuppgifter till individer.[54] Solid vill skapa en effektiv plats

[53] https://www.esamverka.se/download/18.1d126bc174ad1e6c39b6a9/1600695706378/eSam%20-%20MinaData%20v1.0.pdf

[54] Projektet startades av Tim Berners-Lee, känd för att ha uppfunnit World Wide Web, tillsammans med Massachusetts Institute of Technology (MIT).

för individer att hantera sina data och själv påverka hur och var information lagras, vilka människor och organisationer som kan komma åt specifika uppgifter samt hur data ska delas.[55]

Individen sparar och lagrar information i personliga online-datalager, även kallad POD, och individen bestämmer själv var POD:s ska lagras. Individen kan flytta sin information mellan flera POD:s och bestämma vilka applikationer som ska få tillgång till respektive POD. Applikationer som vill hämta information från POD:s måste först autentiseras av Solid. Genom att bestämma vilka uppgifter som lagras i varje POD, var respektive POD lagras och vilka applikationer som har behörighet att använda uppgifterna ges individen fullständig kontroll av sin data.

Figur 2 Personliga online-datalager[56]

POD:s skyddar data med hjälp av regler för åtkomstkontroll. Reglerna kan konfigureras så att individen själv bestämmer exempelvis tidsbegränsningar.

Individen interagerar med systemet antingen genom en domänspecifik applikation eller en webbläsare. Applikationen kan be individen om samtycke till att använda en del av individens data för att ge individen någon form av värde.

[55] https://solidproject.org
[56] Bild från https://solidproject.org

4.3.7 Viktiga egenskaper för individcentrerade dataekosystem

Det finns vissa egenskaper för de individcentrerade dataekosystem som är principiellt viktiga att ta med sig i det fortsatta arbetet. Det handlar bland annat om att dataekosystemet ska:

- tillgodose individens behov av kontroll och insyn,
- möjliggöra för individen att själv lagra information på egen vald plats i ekosystemet,
- ha en aktör som är ansvarig för ekosystemet,
- ha en fungerande infrastruktur som överbryggar interoperabilitetsproblem som grund för datadelning,
- ha ett tydligt regelverk för roller, ansvar, förhållningssätt och behörigheter till ekosystemets olika funktioner.

4.4 Insyn och kontroll i vissa offentliga tjänster

Det finns sedan en tid olika initiativ som syftar till att ge ökad insyn och till viss del även kontroll. Realiseringarna är gjorda tillsammans mellan det offentliga och det privata. Vi väljer att lyfta dessa tre som exempel på när man på olika sätt inom olika sektorer tagit fram lösningar inom området.

4.4.1 Journalen på nätet

E-tjänsten Journalen på nätet, som är åtkomlig via 1177.se, ger individer äldre än 15 år möjlighet att läsa delar av sin journal. Inera AB tillhandhåller och ansvarar för tjänsten som används av mer än 4 miljoner personer.

Journalen på nätet ger individen insyn om vilka uppgifter som hälso- och sjukvården har om dem i syfte att göra patienter mer delaktiga i sin vård och hälsa. Patienter är positiva till att kunna läsa sin journal på nätet och de möjligheter som denna resurs ger. De som använder Journalen på nätet värdesätter möjligheten att få tillgång till provresultat, en översikt över sin hälsa och kontakter med vården samt möjligheteten att följa upp planering och vård efter besöket.[57]

Regioner, kommuner och privata vårdgivare som är offentligt finansierade kan ansluta sig till Journalen på nätet. Tjänsten innehåller till exempel uppgifter som journalanteckningar, tidsbokningar, ordinerade läkemedel och provsvar. Vilka

[57] Moll, J., et al (2018). Patients' Experiences of Accessing Their Electronic Health Records: National Patient Survey in Sweden. *Journal of Medical Internet Research*; 20 (11) 2018.

uppgifter som visas varierar mellan regionerna, men ingen region visar upp all journalinformation för invånarna. Varje vårdgivare väljer dessutom vilken information från deras system som ska göras synlig för individen, vilket leder till variation även inom regionerna.

Individen har direktåtkomst till sina journaluppgifter men har idag inte möjligt att ladda ner eller att dela information vidare med andra aktörer. Utöver det har även individen möjlighet att försegla, det vill säga ta bort möjligheten till direktåtkomst, till hela eller delar av Journalen på nätet för egen åtkomst. Vilket individen kan göra själv eller begära att vården gör det åt hen. Försegling av Journalen på nätet kan även ske på initiativ av vården efter en prövning om informationen anses skada individen, vårdpersonal eller tredje person.

Högsta förvaltningsdomstolen (HFD) konstaterade år 2017 att patientdatalagen (2008:355) enbart tillåter patienten själv att ha direktåtkomst till sin journal.[58] Därmed upphörde möjligheten att ge ombud direktåtkomst till journaluppgifter.

Individen kan begära att få veta om och när vårdpersonal har läst hens journal. I vissa regioner är det möjligt att se loggutdrag direkt i e-tjänsten Journalen på nätet medan det i andra regioner sker i särskild ordning.

4.4.2 minPension

På minPension kan alla som har tjänat in till pension i Sverige logga in och se hela sin pension och göra pensionsprognoser. Verksamheten drivs och finansieras till hälften av staten, till hälften av pensionsbolagen. Det gör minPension till en neutral och oberoende webbportal som är kostnadsfri för användaren. Drygt 30 aktörer inom pensionssektorn levererar information till minPension.

minPension behandlar personuppgifter för att utföra en uppgift av allmänt intresse i samverkan med staten, via Pensionsmyndigheten, och försäkringsbranschen, genom Svensk Försäkring och de anslutna pensionsaktörerna som lämnar pensionsuppgifter till minPension. Pensionsmyndigheten har ett uppdrag att, utifrån den enskildes behov, ge pensionssparare en samlad bild av hela pensionen. Detta uppdrag utförs på frivillig väg genom denna samverkan. minPension har bland annat till uppgift att ge alla

[58] HFD 2017 ref 67.

som tjänar in pension i Sverige en helhetsbild över sin pension, en prognos över den framtida pensionen samt information om vad som påverkar pensionen och vikten av tjänstepension och privat sparande till pension. minPension hämtar in uppgifter från såväl staten som försäkringsbranschen.

Minpension är således ett utmärkt exempel på samarbete mellan privat och offentlig sektor, minPension ger medborgarna mer insyn i vilka uppgifter som ligger till grund för framtida pensioner.

4.4.3 Digital Post

DIGG ansvarar för infrastrukturen för digital post från offentliga aktörer som kallas Mina meddelanden. DIGG är också en av fyra aktörer som tillhandahåller en digital brevlåda. Att ansluta till Mina meddelanden innebär att man godkänner att ta emot digital post från offentliga aktörer som är anslutna till eller kommer att ansluta sig till Mina meddelanden och man kan själv välja om man inte vill ha digital post från vissa avsändare.

Förmedlingsadressregistret (FaR) är grunden för infrastrukturen för digital post. I registret finns information om alla som på något sätt är ansluta till infrastrukturen. Det är mottagare, avsändande offentliga aktörer, förmedlare och brevlådeoperatörer. I samband med att mottagaren skaffar en digital brevlåda sker registrering i FaR och en profil skapas. Profilen som skapas vid registrering innehåller mottagarens personnummer och vilken brevlådeoperatör den valt. Profilen innehåller också information om hur mottagaren vill ta emot meddelanden.

De meddelanden som lagras i en digital brevlåda kan inte begäras ut som allmän handling eftersom den digitala brevlådan är att betrakta som brevlådeinnehavarens eget utrymme.

Eget utrymme[59] är ett juridiskt koncept som har lagts till grund för en rättslig modellösning i e-delegationens vägledning för verksamhetsutveckling inom e-förvaltningen och tillämpas på den statliga brevlådan Min myndighetspost.

[59] För mer information om eget utrymme ur juridiskt perspektiv se bilaga 3, kapitel 4 om eget utrymme

4.5 Exempel på individcentrerade dataekosystem

4.5.1 Hälsa för mig

Hälsa för mig var en satsning som initierades av regeringen år 2012 och som E-hälsomyndigheten (tidigare Apotekens Service Aktiebolag) hade som del av sitt grunduppdrag. I tjänsten skulle det finnas en plats, ett eget utrymme, hos E-hälsomyndigheten för lagring av information, även kallat hälsokonto, som skulle ge individer möjlighet att samla, överblicka och dela sin hälsoinformation. Det personliga hälsokontot skulle vara kostnadsfritt och syftet med satsningen var att stärka individens delaktighet i sin hälsa samt ge individen rätten och möjligheten att förfoga över sina egna hälsodata. Det personliga hälsokontot skulle ge Sveriges invånare möjlighet att livslångt spara, hantera och dela sin hälsodata.

Hälsa för mig skulle utgöras av en plattform där företag och organisationer kunde bygga innovativa och hälsorelaterade tjänster, i form av applikationer, till invånarna. I det personliga hälsokontot skulle individen själv bestämma vilken information som skulle lagras och delas med andra aktörer samt säkerställa informationens korrekthet och kvalitet. Information från hälsokontot skulle bara tillgängliggöras för andra, bortsett från individen själv, efter uttryckligt samtycke av individen. Det skulle göras möjligt genom en samtyckefunktion i tjänsten. Om en applikation anslöts till hälsokontot och individen lämnat ett uttryckligt samtycke till att uppgifter lämnas ut, skulle mottagaren av dessa personuppgifter (det vill säga applikationsleverantören) ansvara för den fortsatta behandlingen av uppgifterna i applikationen.

E-hälsomyndigheten skulle i sitt avtal med appleverantörer ställa krav på att personuppgifter endast skulle få användas enligt gällande personuppgiftslagstiftning och att varje utlämnande av uppgifter skulle föregås av ett samtycke.

Via den infrastruktur som E-hälsomyndigheten var tänkt att tillhandahålla skulle det skapas ett API-baserat ekosystem så att såväl offentliga som privata organisationer skulle kunna erbjuda tjänster där individen skulle ha kontroll och vara i centrum.

Efter rättslig prövning godkände inte Datainspektionen[60] och senare Förvaltningsrätten[61] den tolkning E-hälsomyndigheten hade gjort av de rättsliga förutsättningarna för att genomföra uppdraget.

Datainspektionen konstaterade i en granskning att hälsokontot Hälsa för mig inte uppfyllde dataskyddslagstiftningens krav och utfärdade därför ett antal förelägganden. E-Hälsomyndigheten överklagade beslutet till Förvaltningsrätten i Stockholm som i sin tur avslog överklagandet.

I en dom bedömde Förvaltningsrätten i Stockholm att personuppgiftsansvaret för hälsokontot föll på E-hälsomyndigheten, eftersom det är denne som bestämde den yttre ramen för personuppgiftsbehandlingen och i förlängningen ändamålen med och medlen för behandlingen. Domstolen konstaterade att det inte var fråga om ett s.k. eget utrymme, som vissa myndigheter erbjuder som en slags digital lagringsplats för enskilda. Förvaltningsrätten konstaterade vidare att 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.

Efter förvaltningsrättens dom gjorde E-hälsomyndigheten bedömningen att det rättsliga stödet för hälsokontot inte var tillräckligt och myndigheten valde att inte överklaga domen och avslutade arbetet.

4.6 Sammanfattande slutsats

De individbaserade tjänster som beskrivs ovan är bra exempel som kan betraktas som ekosystem som baseras på samverkan mellan privat och offentlig sektor.

Digital post, minPension, journalen på nätet har alla ett fokus på att ge bättre förmåga för individen till insyn. Det fjärde exemplet, hälsa för mig, hade som målsättning att gå längre än bara insyn genom att även ge individen kontroll över

[60] Tillsyn enligt personuppgiftslagen (1998:204) – E-hälsomyndighetens tjänst Hälsa För Mig, 2017-04-21, dnr 2276-2016.
[61] Förvaltningsrätten i Stockholm, dom 2018-05-24, mål nr 11458-17.

sina uppgifter och möjligheten att dela uppgifter med andra aktörer. Det finns stora utmaningar framförallt legala med att ge individen kontroll av sina uppgifter, inte minst i förhållande till offentliga aktörer, vilket erfarenheter från exemplet hälsa för mig visar.

Tjänsterna är till stor del sektorsvisa lösningar men det finns erfarenheter från alla ovanstående tjänster där frågeställningar kring samverkan offentlig privat sektor, affärsintressen, finansiering, legala frågor, utveckling och förvaltning är intressanta att ta med i ett vidare arbete med utveckling av individbaserade lösningar för insyn och kontroll.

5 Koncepttest Teknisk PoC

Arbetsförmedlingen fick i uppdrag att leda det tekniska arbetet och utvecklingen av den tekniska PoC som nämns i detta regeringsuppdrag.

Arbetsförmedlingens verksamhet syftar ytterst till att effektivt sammanföra arbetsgivare som söker arbetskraft med arbetssökande som söker arbete, prioritera och rusta dem som befinner sig långt från arbetsmarknaden samt bidra till att stadigvarande öka sysselsättningen på lång sikt.

Utvecklingen går idag fort inom flera områden och tekniska innovationer förändrar och utvecklar även arbetsmarknaden. I framtagandet av denna PoC har vi utgått från att kunderna har en vilja att själva kunna agera – att ha kontroll över sin situation. Den arbetssökande vill hitta ett jobb och arbetsgivaren vill hitta rätt arbetskraft.

Framtaget förslag på teknisk PoC tar sin utgångspunkt i dagens situation och utforskar de förutsättningar och möjligheter som finns idag.

5.1 Livshändelse: gå till arbete

Att utgå från en livshändelse handlar om att identifiera behov, oavsett ansvarig myndighet/organisation, bland medborgarna som offentlig sektor är till för att möta. En livshändelse beskriver något som inträffar i en människas liv och som medför att livssituationen ändras vilket kan innebära ett digitalt eller analogt möte med offentlig sektor. Livshändelsen g*å till arbete* är mycket komplex och mängden aktiviteter, insatser, myndighetsrelationer och aktörer är många. Målgruppen som står inför arbetslöshet och ett arbetssökande är differentierad och kräver olika typer av kontakter utifrån individuell förutsättning. Arbetsförmedlingen har i arbetet med koncepttest valt att fokusera på en avgränsad del av denna livshändelse som handlar om att söka arbete.

5.2 Beskrivning av Koncepttest (PoC)

Utgångsläget har varit att utveckla Arbetsförmedlingens e-tjänst Min profil med ny funktionalitet i förhållande till befintlig lagstiftning och gällande rätt inom ramen för regeringsuppdraget.

Målsättningen med koncepttestet är att visa hur möjlighet till insyn och kontroll över data om individen hos offentlig, och i förlängningen, privat sektor kan ge tydliga mervärden för individen. Integritet och egen hämtning och delning har utgjort kärnan i framtagen PoC, och därmed också de juridiska förutsättningarna

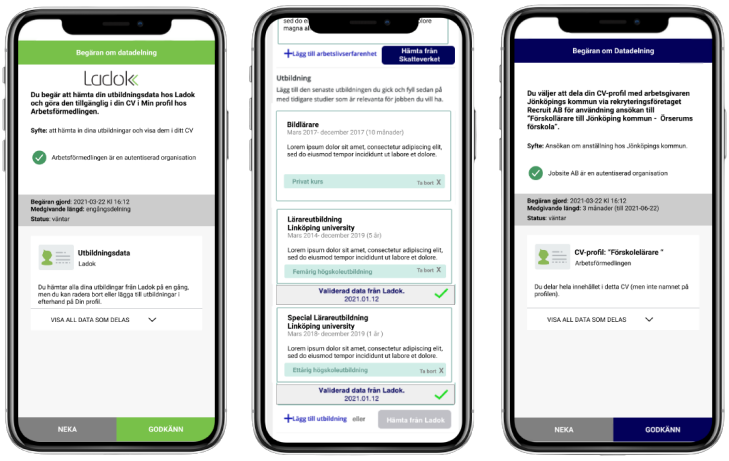
för att hantera och dela personliga data[62]. PoC:en visar hur en individ kan hämta data från några utvalda myndigheter och organisationer för att (hos AF) kunna skapa ett CV med validerade uppgifter/data från validerad källa som sedan kan användas för att underlätta arbetssökande.

Levererad PoC är inte ett färdigt system som är klart att driftsätta. Framtagen PoC är att se som en utforskande testimplementation. Implementationen[63] är en CV-tjänst som integreras mot ett begränsat antal myndigheter och aktörer.

Kort beskrivning av framtaget scenario: *Anna söker jobb som förskollärare, och delar sitt CV från Arbetsförmedlingen med många jobbsajter. Hennes CV innehåller validerade data från olika myndigheter, bland annat körkort, folkbokföringsadress, och studieintyg.*

Målsättningen med framtaget lösningsförslag är att Anna genom lösningen ska kunna begära ut/hämta validerad information från myndigheter som är nödvändig inom ramen för hennes arbetssökande och få en utökad möjlighet att överföra uppgifter mellan aktörer i olika sammanhang. Detta skapar en trovärdighet för uppgifterna för läsare och skapar förutsättningar för Anna att effektivera sin ansökningsprocess.

Figur 3 Vyer av ansökningsprocess

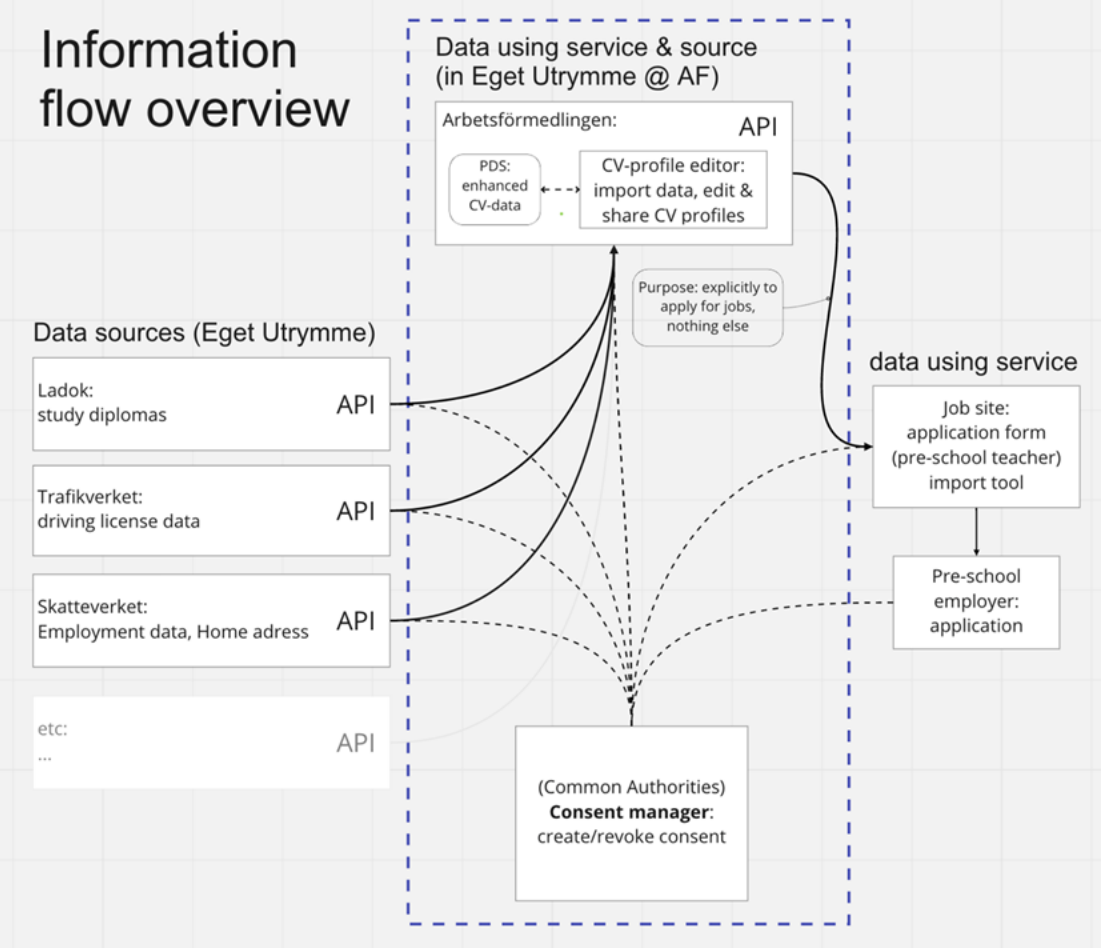


[62] Se Bilaga 3 *Övergripande juridisk analys av möjligheterna att öka insynen och kontrollen för individer*

[63] Inom ramen för uppdraget har vi inte tagit fram en generell modell för säkerhets och integritetsfrågor, som till exempel hur en generell operator ska hantera & definiera vilka 3:e part tjänster som är pålitliga att dela data till.

Detta utlämnande som sker inom ramen för denna PoC (från utpekade myndigheter – se bild) på begäran av den enskilda (Anna) och till ett eget utrymme får anses förenligt med gällande rätt så länge sekretess inte gäller för uppgifterna i förhållande till den enskilda och ett elektroniskt utlämnande får och kan ske säkert. Modellen behöver, utifrån gällande rätt, således kräva att den enskilde vidtar en viss åtgärd som kan anses motsvara en begäran innan uppgifterna visas eller överförs.

Figur 4 Dataflöden i koncepttestet



5.3 Informations- och IT-säkerhet

Att kunna utbyta information mellan myndigheter, kommuner, fristående aktörer, landsting/regioner, arbetsgivare med flera ställer höga rättsliga krav. Arbetsförmedlingen har i denna tekniska PoC arbetat systematiskt med informations- och IT-säkerhet för att säkerställa att både individ och den

information som behandlas, har ett adekvat skydd samt att styrande författningar och regelverk efterlevs.

Informationssäkerhet omfattar per definition konfidentialitet, riktighet och tillgänglighet samt spårbarhet för information men handlar också om ansvar, riskmedvetenhet och helhetssyn. Området är komplext och innefattar utöver tekniska säkerhetslösningar även säkerhetsrelaterade lösningar inom exempelvis administrativ- och personalsäkerhet. Utöver dessa finns naturligtvis även ekonomiska och legala aspekter att ta hänsyn till.

I och med att vi idag lever i ett informationssamhälle där större mängder information än någonsin tidigare bearbetas, lagras, kommuniceras och mångfaldigas måste informationssäkerhet ses som en förutsättning, för att nya företeelser i samhället ska kunna fungera på ett säkert sätt. Det måste därvid framhållas vikten av att medborgare och företag kan känna tillit till myndigheternas sätt att hantera information.

I Arbetsförmedlingens arbete med denna PoC har följande områden relaterade till informations- och IT-säkerhet berörts:

I vilket syfte och med vilken rätt utbyts informationen: Vem har rätt att ta del av vilken information och på vilket sätt?

Hantering av information för annans räkning: En digital infrastruktur i vilken myndigheter och andra aktörer samarbetar genom att använda samma tekniska komponenter kan medföra att myndigheten hanterar information åt andra. Sådan hantering kan innebära både bearbetning, lagring och förmedling, det vill säga hantering av mer varaktig karaktär eller tillfällig hantering.

Offentlighet och sekretess vid informationsutbyte: Information hos en myndighet omfattas av bland annat av bestämmelserna i offentlighets- och sekretesslagen (2009:400), innebärande att en myndighet är ålagda skydda uppgifter som omfattas av sekretess det vill säga ej delge eller röja sådana uppgifter som lagstiftaren avser skydda, till obehörig.

Personuppgiftsansvar vid informationsutbyte: Vem som är personuppgiftsansvarig och vem som är personuppgiftsbiträde vid behandling av personuppgifter i arkitekturen ska vara utredd.

Specifika informations- och IT-säkerhetsrelaterade krav vid test av denna PoC redovisas för i bilaga 5 *Fördjupad beskrivning av koncepttest.*

5.4 Rättsliga förutsättningar för PoC:

De rättsliga förutsättningarna för e-tjänsten utgår i allt väsentligt från den generella rättsliga beskrivningen som återfinns i bilaga 4 *Övergripande juridisk analys av möjligheten att öka insynen och kontrollen för individer*

Upplägget i PoC utgår från att:

- Individen har ett Eget Utrymme hos de myndigheter som är aktuella i denna PoC.
- Myndigheten har Personuppgiftsansvar för innehållet, trots att den inte har rätt att läsa innehållet i utrymmet, och detta begränsar hur utrymmet får användas och hur data delas med tredje part.
- Individen kan själv bearbeta och tillföra information i det Egna Utrymmet.
- Endast myndigheter kan tillhandahålla Egna Utrymmen (i enlighet med förutsättningarna för endast teknisk bearbetning och lagring i 2:13 TF. Det går att utkontraktera men då agerar tredje parten som en förlängd arm av myndigheten.
- Endast individen har tillgång till innehållet (nyttoinformationen). Myndigheten får inte ta del av nyttoinformationen. Som myndighet får vi endast tillgång till drifts- och säkerhetsrelaterad information.

5.4.1 Min profil utökas med ny funktionalitet

Utgångsläget har varit att, som tidigare nämnts, utveckla Arbetsförmedlingens e-tjänst Min profil med ny funktionalitet i förhållande till befintlig lagstiftning och gällande rätt.

Min profils nya funktionalitet syftar till att erbjuda en service, som är helt frivillig, för enskilda som söker arbete så att de på ett effektivt sätt kan utforma ett CV som innehåller producentens data genom egen hämtning. Möjlighet ska också finnas för den enskilde att dela sitt färdigställda CV med arbetsgivare eller rekryteringsföretag. Dessa benämns fortsättningsvis som tredje part. Det ska vidare finnas en möjlighet att skicka CV:t till Arbetsförmedlingens

mottagningsställe[64] i syfte att ett ärende[65] enligt förvaltningslagen ska kunna inledas. Dessa behandlingar kommer framgent att benämnas *den nya funktionaliteten.*

Inga känsliga personuppgifter i enlighet med EU:s dataskyddsförordning[66] eller särskilt skyddsvärda i enlighet med Arbetsförmedlingens registerlagar kommer att behandlas inom ramen för den nya funktionaliteten.

5.4.2 Eget utrymme

Den enskilde får tillgång till den nya funktionaliteten via ett så kallat eget utrymme. Detta innebär att Arbetsförmedlingen tillhandahåller tjänsten endast som ett led i teknisk bearbetning och lagring för annans räkning[67] Ett eget utrymme kan beskrivas som en insynsskyddad elektronisk plats som bara användaren har åtkomst till.

5.4.3 Legalitet

En myndighet får endast vidta åtgärder som har stöd i rättsordningen.[68] Det behöver således finnas ett rättsligt stöd för Arbetsförmedlingen att erbjuda denna funktionalitet. Vid bedömningen av legalitetsprincipens inverkan på Arbetsförmedlingens möjligheter att tillhandahålla aktuell ny funktionalitet måste syftet med tjänsten kopplas till Arbetsförmedlingens uppdrag.

I Arbetsförmedlingens instruktion framkommer det att myndigheten har att verka för att förbättra arbetsmarknadens funktionssätt genom att effektivt sammanföra dem som söker arbete med dem som söker arbetskraft.[69] I regleringsbrevet för 2021[70] framgår att i förberedelsearbetet inför Arbetsförmedlingens stundande reform ska myndigheten särskilt utveckla den digitala infrastruktur som är nödvändig för ett effektivt utbyte av information mellan berörda aktörer i den arbetsmarknadspolitiska verksamheten. En e-tjänst som syftar till att stötta den enskilde i sitt framtagande av ett CV som innehåller data från producenten, med

[64] En funktion hos Arbetsförmedlingen där elektroniska handlingar mottas, ankomstregistreras, diarieförs och i vissa fall kvitteras.
[65] Visualisering av detta ingår ej i POC
[66] EU:s dataskyddsförordning art 9
[67] enligt 2 kap 13 § tryckfrihetsförordningen (1949:105
[68] SOU 2018:25, s. 280
[69] 2 § Förordning (2007:1030) med instruktion för Arbetsförmedlingen Arbetsförmedlingen ska verka för att förbättra arbetsmarknadens funktionssätt genom att 1. effektivt sammanföra dem som söker arbete med dem som söker arbetskraft
[70] https://www.esv.se/statsliggaren/regleringsbrev/?rbid=21825

möjlighet att dela med tredje part, får således anses rymmas inom myndighetens uppdrag. I förlängningen ökar effektiviteten på arbetsmarknaden på grund av snabbare rekryteringsprocesser.

5.4.4 Behandlingar som sker i den nya funktionaliteten

- Egen hämtning som initieras av individen för att påbörja CV:t.
- Möjlighet till redigering av CV, i de delar som inte är validerade.
- Egen delning som initieras av individen när CV:t är färdigt.

5.4.5 Personuppgiftsansvar

Mot bakgrund av att personuppgiftsansvaret i eget utrymme aldrig har prövats i högre instans är det inte helt enkelt att besvara vilken part som bär personuppgiftsansvaret för de uppgifter som behandlas. Utifrån den praxis som har utvecklats beträffande andra digitala tjänster så kan möjligen det rådande rättsläget preciseras. Beträffande personuppgiftsbehandling som förekommer i myndighetens verksamhetssystem, vilket är utanför eget utrymme är det relativt oproblematiskt att konstatera att myndigheten är personuppgiftsansvarig. I dessa fall är det myndigheten som bestämmer ändamål och medel för personuppgiftsbehandlingen.

Att bedöma personuppgiftsansvarets placering beträffande digitala tjänster med eget utrymme är i avsaknad av klargörande praxis förenat med vissa svårigheter. Det har även visat sig att det saknas tydliga riktlinjer som underlättar för myndigheter att bedöma personuppgiftsansvarets placering.[71]

Den som ensamt eller tillsammans med andra bestämmer ändamål och medel för en behandling av personuppgifter är, enligt EU:s dataskyddsförordning, personuppgiftsansvarig för behandlingen.[72] I Sverige regleras myndigheters personuppgiftsansvar dessutom ofta i en registerförfattning som gäller för det område av myndighetens personuppgiftsbehandling som registerförfattningen reglerar. Arbetsförmedlingen är enligt 3 § lag (2002:546) om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten, Af-PUL personuppgiftsansvarig för den behandling som Arbetsförmedlingen utför.

[71] SOU 2018:25 s. 288
[72] Artikel 4.7 dataskyddsförordningen

Det är mycket som talar för att det är myndigheten som upprättat en digital tjänst med eget utrymme som bestämmer ändamål och medel för personuppgiftsbehandlingen i eget utrymme. Ansvaret borde omfatta både nyttoinformation samt personuppgifter som anknyter till driften och säkerheten av eget utrymme. Enligt vår mening finns stöd för en sådan uppfattning vid beaktande av Högsta förvaltningsdomstolens dom HFD 2012 ref. 21. Rättsfallet ger uttryck för en helhetssyn på personuppgiftsansvaret som principiellt innebär ett långtgående ansvar. I rättsfallet var det inte den personuppgiftsansvariga som hade skapat de tekniska förutsättningarna, istället hade den personuppgiftsansvariga endast hänvisat till vissa tekniska tjänster. Detta hindrade dock inte domstolen från att betrakta Försäkringskassan som personuppgiftsansvarig.

Vad gäller omständigheterna som omgärdar eget utrymme har myndigheten i dessa fall inte bara tagit initiativ till personuppgiftsbehandlingen utan myndigheten har även skapat de tekniska förutsättningarna för tjänsten. Detta talar än starkare för att myndigheten är ensamt personuppgiftsansvarig vad gäller personuppgifter i eget utrymme.

Mot bakgrund av att dataskyddsförordningen nyligen trädde i kraft saknas det praxis på området och rättslitteraturen är sparsam. Vad beträffar Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (dataskyddsdirektivet), som är dataskyddsförordningens föregångare, så framstår definitionen av personuppgiftsansvarig som näst intill identisk med art. 4 (7) dataskyddsförordningen. Detta gäller även PuL som införlivats i svensk rätt utifrån dataskyddsdirektivet.[73] Samma likheter finns även i andra delar av dataskyddsförordningen som exempelvis definitionen för personuppgifter och behandling av sådana uppgifter. Detta innebär att tidigare avgöranden från svenska domstolar kommer att beaktas. Att svensk domstol eller EU-domstolen drastiskt skulle förändra den praxis som utarbetats håller vi för mindre sannolikt.

Arbetsförmedlingen bestämmer i den nya funktionaliteten ändamålet med behandlingen av personuppgifterna, det vill säga möjligheten att skapa ett CV som

[73] Se Dataskyddsdirektivet art. 2 (a) och personuppgiftslag (1998:204) 3 §

innehåller data från validerad källa. Arbetsförmedlingen har också bestämt medlen för behandlingen av personuppgifter genom att anvisa de tekniska överföringsmöjligheter som erbjuds som gäller för egen hämtning och egen delning. Det är därutöver Arbetsförmedlingen som beslutar att denna funktionalitet ska inrättas inom ramen för ett eget utrymme och vilken utformning detta ska ha, vilka säkerhetsnivåer som ska gälla, vilka möjligheter som ska finnas för att inhämta uppgifter och lämna ut uppgifter samt vem som ska svara för drift och förvaltning. Det är vidare Arbetsförmedlingen som ställer upp villkor för användningen av det egna utrymmet och som har möjlighet att tillgodose de rättigheter som tillkommer den enskilde.

Arbetsförmedlingen är personuppgiftsansvarig för såväl den hämtning av uppgifter (överföring) som sker som den delning av uppgifter som görs fram till dess att uppgifterna mottas av extern part då det är Arbetsförmedlingen som tillhandahåller ändamål och medel för dessa överföringar, oaktat att denna behandling sker innan uppgifterna (eventuellt) inkommer till myndigheten.

Med personuppgiftsansvaret följer skyldigheter för den ansvarige såsom exempelvis att informera den registrerade, att skydda uppgifterna från obehörig åtkomst, att tillse att inte fler uppgifter än nödvändigt behandlas och att behandlingen inte pågår längre tid än nödvändigt. Den personuppgiftsansvarige måste också respektera den registrerades rättigheter såsom rätt till rättelse, rätt att få uppgifter raderade, rätt att få del av vilka uppgifter som finns registrerade genom s.k. registerutdrag osv. Dessutom har den registrerade rätt till ersättning om personen lidit materiell eller immateriell skada till följd av en överträdelse av dataskyddsförordningen som den personuppgiftsansvarig medverkat till. Exempelvis om den tekniska utformningen medför att personuppgifter lagras längre än berättigat och den enskilde där av skulle lida skada.

Samtliga rättigheter som tillkommer en användare av den nya funktionaliteten måste dessutom kunna efterlevas av personuppgiftsansvarig utan att myndigheten själva får insyn i det egna utrymmet, i syfte att statusen av utrymmet ska kunna upprätthållas.

5.4.5.1 Personuppgiftsansvarets räckvidd

Med personuppgiftsansvaret följer, enligt ovan, ett antal skyldigheter som den personuppgiftsansvarige måste efterleva. Fråga är om myndigheten har möjlighet att efterleva dessa skyldigheter. I det följande kommer vi på ett generellt plan

redogöra för den problematik som anknyter till personuppgiftsansvaret i relation till hur en digital tjänst med eget utrymme upprättas.

Det finns en möjlighet att handlingar i eget utrymme inte betraktas som allmänna om handlingarna förvaras endast som led i teknisk bearbetning eller teknisk lagring för annans räkning. Detta förutsätter dock att digitala tjänster med eget utrymme får en särskild utformning. Exempelvis ska nyttoinformationen vara avgränsad från myndighetens IT-miljö, åtminstone logiskt från myndighetens verksamhetssystem. Dessutom ska myndighetens personal som regel inte ha åtkomst till informationen i eget utrymme. Informationen ska således vara förbehållen användaren.

Mot denna bakgrund är det inte givet att myndigheten kan kontrollera att personuppgifter behandlas på ett sätt som är förenligt med dataskyddsförordningen. Digitaliseringsrättsutredningen har exempelvis ifrågasatt hur en myndighet kan säkerställa att privatpersoner endast för in adekvata och relevanta personuppgifter i förhållande till ändamålet för personuppgiftsbehandlingen.[74]

Utformningen av eget utrymme bygger på att myndighetens personal inte ska ha åtkomst till informationen i eget utrymme, endast i undantagsfall ska sådan åtkomst finnas. Som personuppgiftsansvarig föreligger även en skyldighet att på den registrerades begäran lämna ut ett registerutdrag vilket framgår av dataskyddsförordningen art. 15. Registerutdraget ska innehålla information om de behandlingsåtgärder som den personuppgiftsansvarige vidtar med personuppgifterna. Bland annat ska det framgå för vilket ändamål som personuppgifterna behandlas. Vidare ska den personuppgiftsansvariga enligt dataskyddsförordningen art. 16 och art. 17 under vissa förhållanden radera eller rätta personuppgifter när den registrerade begär detta.

Ovan skyldigheter visar att en myndighet i rollen som personuppgiftsansvarig måste fastställa rutiner av tekniska och organisatorisk beskaffenhet för att dataskyddsförordningen ska kunna efterlevas. Dessa rutiner är omfattande till sin karaktär och fråga är om myndigheten måste ha åtkomst till informationen i eget utrymme för att kunna utöva sitt ansvar.

[74] SOU 2018:25 s. 290

Som personuppgiftsansvarig inträder en rad skyldigheter gentemot den registrerade. Exempelvis får endast personuppgifter behandlas utifrån ett särskilt ändamål och personuppgifter ska i vissa fall raderas och rättas om den registrerade begär det. I och med detta kan det ifrågasättas om undantaget i 2 kap. 13 § TF över huvud taget kan tillämpas eftersom skyldigheterna enligt dataskyddsförordningen är så pass ingripande. En förutsättning för att eget utrymme ska kunna fylla sin funktion är att handlingarna som förvaras i utrymmet förblir användarens egna och inte kan nås av andra.

För att en myndighet fullt ut ska kunna kontrollera att endast personuppgifter behandlas i eget utrymme för ett visst ändamål torde det kanske krävas att myndigheten har viss åtkomst. I detta fall finns det en motsättning mellan förutsättningarna för eget utrymme och de skyldigheter som följer av personuppgiftsansvaret vilket i sådana fall medför att EU:s dataskyddsförordning står i potentiell konflikt med grunden för det egna utrymmet Om myndigheten dock genom tekniska begränsningar och tydliga användarvillkor lyckas stävja missbruk och på så vis säkerställa att endast den information som är nödvändig för ändamålet behandlas torde inte denna motsättning finnas.

Det är denna ambition som vi har i denna PoC, det vill säga det ska i högst möjliga mån vara förvalda svarsalternativ och i den mån fritextfält anses vara nödvändigt för ändamålet ska det vara tydligt för den enskilde vad fältet ska användas till, vilket tydliggörs i exempelvis användarvillkor. Det ska finnas tekniska begränsningar på plats så att den enskilde inte antecknar sådana uppgifter som inte är adekvata och relevanta eller tillåtna. Arbetsförmedlingen förebygger detta genom att ha tydliga riktlinjer (användarvillkor) för vad som får antecknas i fritextfältet och tekniska begränsningar (spamfilter, vid uppladdning av filer begränsa storlek, format). Omedelbar gallring ska ske när inadekvata och irrelevanta uppgifter mot förmodan matas in.

Genom att aktivt arbeta med *privacy by design* vet myndigheten vilken personuppgiftsbehandling som de facto sker i det egna utrymmet utan att behöva ta del av nyttoinformationen. Därutöver får Arbetsförmedlingen ha insyn i den drifts- och säkerhetsrelaterade informationen vilken inkluderar metainformation. Myndigheten kan på så vis detektera visst missbruk utan att behöva ta del av nyttoinformationen.

Naturligtvis skulle Arbetsförmedlingen kunna undgå många av de skyldigheter som stadgas i dataskyddsförordningen om användaren istället betraktas som personuppgiftsansvarig för nyttoinformationen i eget utrymme. Alltjämt föreligger en osäkerhet kring placeringen av personuppgiftsansvaret och med en välvillig tolkning kanske användaren kan betraktas som personuppgiftsansvarig i enstaka fall. Enligt vår mening finns det dock anledning att kritisera en sådan tolkning.

5.4.6 Samordnad behandling

Arbetsförmedlingens personuppgiftsansvar upphör när den enskildes uppgifter når tredje parts ansökningsformulär enligt bild x i de tekniska skisserna. Tredje part blir personuppgiftsansvarig för uppgifterna först i ansökningsformuläret och behandlar inga personuppgifter i den nya funktionaliteten. Det är alltså fråga om ett utlämnande från en PuA (Arbetsförmedlingen) till en annan (tredje part), så kallad samordnad behandling. Detta gäller även om delning görs på den enskildes initiativ. Vid samordnad behandling är det inte ett krav på ett inbördes arrangemang som vid ett gemensamt personuppgiftsansvar (artikel 26 dataskyddsförordningen), s.k. datadelningsavtal. Däremot kan det vara lämpligt med någon form av överenskommelse även vid samordnad behandling.[75]

Normalt sett bör den utlämnande aktören i vart fall försäkra sig om att personuppgifterna inte behandlas i strid med EU:s dataskyddsförordning av den mottagande aktören. Den mottagande aktören bör i sin tur i vart fall försäkra sig om att de registrerade fått korrekt information om utlämnandet och att insamlandet i övrigt var lagligt. Detta kan i förlängningen innebära ett behov av koordinerad hantering av registrerades utövande av sina rättigheter, informationslämning, reglering avseende säkerhetsåtgärder osv. Skillnaden jämfört med ett inbördes arrangemang enligt artikel 26 EU:s dataskyddsförordning förefaller därmed inte som särskilt stor. De allmänna villkoren kan ur dataskyddsynpunkt inrymma en överenskommelse som reglerar utlämnandet från en personuppgiftsansvarig till en annan (Arbetsförmedlingen till arbetsgivare/rekryteringsföretag). Det som bör regleras i de allmänna villkoren är; vilka ändamål som personuppgifterna får hanteras för, vem som informerar den registrerade om vad med mera.

[75] jmf. Kahn Pedersen, http://kahnpedersen.se/wp-content/uploads/2017/12/Johan_Kahn-Fredrik_Gustafsson.pdf;

5.4.7 Laglig grund för de behandlingar som sker i tjänsten

Arbetsförmedlingens behandling av personuppgifter regleras, förutom av dataskyddsförordningen och lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) även av lagen (2002:546) om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten (AF-PUL) och förordningen (2002:623) om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten (AF-PUF).

Arbetsförmedlingen tillhandahåller en funktionalitet i syfte att underlätta för enskilda att söka arbete och för arbetsgivare att hitta arbetskraft. Det får anses ligga inom det allmänna intresset (art 6 e i EU:s dataskyddsförordning) att Arbetsförmedlingen tillhandahåller (som en service) ett effektivt sätt för sina kunder att komma i kontakt med varandra genom det specifika ändamålet att den enskilde på ett effektivare sätt ska kunna publicera ansökningar om anställning.

I förarbetena till dataskyddslagen[76] samt i skäl 45 till EU:s dataskyddsförordning framkommer att förordningen inte medför något krav på en särskild lag för varje enskild behandling, utan att det kan räcka med en lag som grund för flera behandlingar om behandlingen krävs för att utföra en uppgift av allmänt intresse. Det krävs således inte att varje behandling som utförs i den aktuella e-tjänsten finns fastställd i nationell rätt. Den personuppgiftsbehandling som sker i utrymmet får dessutom anses utgöra en del av den arbetsmarknadspolitiska verksamheten mot bakgrund av att begreppet arbetsmarknadspolitisk verksamhet har ett mycket omfattande tillämpningsområde[77]. Ändamålet för behandlingen måste således finna stöd i myndighetens registerlag AF-PUL. Ändamålet att sätta samman ett CV som innehåller validerade data för delning till andra aktörer avser publicering av ansökningar om anställning enligt 4 § punkten 2 AF-PUL. Med ansökningar om anställning förstås sådana handlingar eller uppgifter som

[76] Prop 2017/18:105 sid. 49.

[77] I förarbeten till AF-PuL har regeringen preciserat när lagen typiskt sätt ska tillämpas. Enligt regeringen ska lagen b.la. tillämpas när personuppgifter om en arbetssökande, en arbetsgivare eller en kontaktperson behövs för att genomföra den verksamhet som Arbetsförmedlingen har i uppdrag att bedriva.[1] Denna personkrets kan dock utökas under förutsättning att behandlingen av personuppgifter sker i den arbetsmarknadspolitiska verksamheten.[2] Enligt förarbeten till AF-PuL framgår det att registerlagen inte ska tillämpas när personuppgifter behandlas inom den interna administrationen som ligger utanför den direkta kärnverksamheten.[3] Utanför tillämpningsområdet hör exempelvis frågor som gäller personal, uppgift om till vilken enhet inom en myndighet ett ärende hör, uppgift om vem som handlägger ett visst ärende eller uppgift om vilka specialkunskaper en handläggare besitter.

normalt ingår i en ansökan om anställning, till exempel kontaktuppgifter, meritförteckning och personligt brev. I 3 a § AF-PUF specificeras vilka personuppgifter som får behandlas för detta ändamål, se exempelvis; uppgifter om körkort, utbildning och tidigare arbetsgivare. Enligt andra stycket får personuppgifterna behandlas för publicering av ansökningar om anställning endast om den arbetssökande har samtyckt till behandlingen. Samtycket i 3 a § AF-PUF är en så kallad integritetshöjande åtgärd och ska inte ses som en rättslig grund.

Den arbetssökande har rätt att när som helst återkalla ett lämnat samtycke och vid ett återkallande får personuppgifterna inte längre behandlas för publicering av ansökningar om anställning. Ett återkallat samtycke enligt 3 a § innebär att samtycket endast kan återkallas när det gäller behandlingen i e-tjänsten (vilket är en behandling under en väldigt kort tid). Därefter har uppgifterna anlänt till tredjepartsaktören (arbetsgivaren/rekryteringsföretaget). När informationen väl har nått tredjepartsaktören kan ett återkallande av samtycket aldrig omfatta informationen hos denne. De har då tagit över personuppgiftsansvaret. När en återkallelse av samtycket har gjorts och kommit till myndighetens kännedom får ytterligare personuppgifter om den enskilde inte behandlas. Behandlingen av redan insamlade uppgifter får dock fortsätta. Det ska finnas funktioner i tjänsten som kan upprätthålla detta. Den samling personuppgifter som behandlas i det egna utrymmet utgörs inte av en arbetsmarknadspolitisk databas enligt 7 § AF-PUL då personuppgifterna *inte används gemensamt i verksamheten* för de ändamål som anges i 4–6 §§ samma lag. Arbetsförmedlingen ska tillämpa EU:s dataskyddsförordning vid behandling av personuppgifter utanför den arbetsmarknadspolitiska databasen. Dessutom ska Arbetsförmedlingen tillämpa de kompletterande bestämmelserna i 1-6 §§ Af-PUL samt den kompletterande dataskyddslagen.

5.4.8 Alternativ laglig grund specifikt för behandlingarna egen hämtning och egen delning

Arbetsförmedlingen får anses ha tillräckligt med stöd för behandlingen *lagring* i den nya funktionaliteten. Det kan tänkas att det allmänna intresset inte kan anses täcka in själva överföringen av personuppgifter till och från det egna utrymmet. Samtycke i enlighet med artikel 6.1 a i EU:s dataskyddsförordning skulle kunna utgöra en alternativ laglig grund för personuppgiftsbehandlingarna egen hämtning och egen delning i tjänsten, det vill säga endast själva överföringen av personuppgifter till och från det egna utrymmet. Det ska understryka att

samtycke som rättslig grund inte under några omständigheter får ersätta eller överlappa en mer lämplig rättslig grund som vi bedömer vara det allmänna intresset enligt ovan.

Myndigheters utrymme att grunda behandling på samtycke från den registrerade är väldigt begränsat. Men med avseende på e-tjänstens och behandlingens art och beskaffenhet utgör sannolikhetsgraden för att den enskilde faktiskt frivilligt har lämnat ett samtycke till behandlingen som förefallande högt. Den enskilde har en genuin och fri valmöjlighet att använda den nya funktionaliteten då användandet av den är *helt frivillig*. Den enskilde kan helt utan konsekvenser avstå från att använda funktionaliteten eller ta tillbaka sitt samtycke. Det får således i vart fall inte anses som osannolikt att samtycke har lämnats på sådan frivillig basis som stadgas i skäl 42 EU:s dataskyddsförordning[78]. Även om behandlingen överföring vid egen hämtning och delning kan tänkas ske med den rättsliga grunden samtycke så innebär inte detta att den personuppgiftsansvariges ansvar upphör utan samtycket utgör då den lagliga grunden för personuppgiftsbehandlingen och är giltig under de förutsättningar som framgår av dataskyddsförordningen.

Om samtycke används är det viktigt att dokumentera att samtycke har givits och säkerställa att det sparas på behörigt ställe (på motsvarande sätt som information för det egna utrymmet). Loggar får hämtas och lagras inom myndighetens informationstillgångar för att säkerställa gallring eller radering enligt gallringsbeslut. Viktigt är att komma ihåg att dokumentation av samtycke sker för myndighetens räkning och blir således allmän handling när det inkommer till myndigheten.

5.4.9 Egen hämtning av uppgifter till det egna utrymmet

Att Arbetsförmedlingen är personuppgiftsansvarig för innehållet i det egna utrymmet, begränsar hur utrymmet får användas och hur uppgifter kan delas med

[78] Den enskilde är på intet sätt tvungen att lämna samtycke och kommer inte att förlora några positiva effekter och slipper även negativa konsekvenser om samtycket inte skulle lämnas. Separata samtycken ska ges för de olika ändamålen egen hämtning och egen delning. Samtycket är informerat då information ges om att det är Arbetsförmedlingen som är personuppgiftsansvarig, ändamålen för behandlingen, vilka uppgifter som kommer registreras och behandlas samt rätten att återkalla ett lämnat samtycke.

tredje parter. Det är Arbetsförmedlingen som sätter upp förutsättningarna för hur informationen får hanteras så att tillämpliga regler om dataskydd kan efterlevas.

Anna har i den nya funktionaliteten möjlighet att inhämta data som är *nödvändig inom ramen för hennes arbetssökande som förskollärare.* Anna slipper själv mata in informationen och leta upp/inhämta dokumentation som stödjer uppgifterna. Data blir dessutom validerad då den inhämtas direkt ifrån ursprungskällan.

Den tekniska utformningen av egen hämtning sker i två steg. Först sker ett utlämnande från berörd myndighets verksamhetssystem till ett eget utrymme (Annas) som tillhandahålls av denna myndighet[79]. Därefter tillhandahåller den nya funktionaliteten en integration för hämtning från det egna utrymmet hos denna myndighet till Annas egna utrymme hos Arbetsförmedlingen. Funktionen utformas så att uppgifterna kan inhämtas först efter en *uttrycklig begäran* från Anna samt att endast de uppgifter som är nödvändiga *för ändamålet inhämtas* och inte rör någon annan än *Anna, som skickat en begäran.* Det spelar ingen roll om den data som inhämtats och som ingår i delningen endast är kopierad och endast visas upp i e-tjänsten hos Arbetsförmedlingen. Uppvisande av information är också en behandling som Arbetsförmedlingen ansvarar för (enligt the once only principle). Det kan finnas fördelar med att informationen endast visas upp, då det reducerar antalet lagrade kopior (uppgiftsminimering).

Funktionaliteten kan å andra sidan begränsas då en enskilde eventuellt inte kan bearbeta informationen på önskvärt sätt. I enlighet med 2 kap 31 § andra punkten skollagen (2010:800) ska Anna visa upp utdrag ur belastningsregistret original innan hon erbjuds anställning. Uppgifter som rör lagöverträdelser är inte känsliga personuppgifter i dataskyddsförordningens mening men dessa uppgifter är särskilt skyddsvärda enligt artikel 10. Skyldigheten att visa registerutdrag gäller oavsett om verksamheten bedrivs av offentlig eller enskild huvudman. Kravet på registerkontroll är lagstadgad utöver skollagen i lagen (2013: 852) om registerkontroll av personer som ska arbeta med barn. Bestämmelser finns även i lagen (1998:620) om belastningsregister. Arbetsförmedlingen ska inte inom ramen för den nya funktionaliteten tillhandahålla en funktion att hämta och dela Annas eventuella belastningsregister då det inte finns ett lagligt stöd för denna

[79] Se vidare avsnitt 2.1 i bilaga 2

behandling. Registerutdraget ska dock lämnas till den inom den anställande verksamheten som beslutar om att anlita eller ta emot Anna som förskolelärare. Anna ska dock inte skicka med denna uppgift, via den nya funktionaliteten utan direkt till arbetsgivaren när det blir aktuellt (utan Arbetsförmedlingens försorg).

5.4.10 Utlämnande/egen delning till tredje part

Egen delning till tredje part kan bara ske med ett ändamål som faller inom ramarna för myndighetens uppdrag och med ett tydligt medgivande från Anna. Ett utlämnande ska således alltid ske genom en aktiv handling där Arbetsförmedlingen i aktuellt tillhandhåller förutsättningarna för det. Möjligheterna att dela information från ett eget utrymme med andra parter kan ske först när det är säkerställt att detta får ske utifrån ett dataskyddsperspektiv.

Utlämnande från det egna utrymmet kan inte anses innebära konsekvenser för myndigheten utifrån TF:s reglering om allmänna handlingar. Någon sekretessproblematik bedöms inte heller uppkomma, då det inte kan anses vara myndigheten som lämnar ut handlingar från individens egna utrymme.

För det fall att det skulle anses ske en expediering i enlighet med tryckfrihetsförordningen när informationen lämnas ut från det egna utrymmet, går informationen från att vara föremål för sekretess enligt 40:5 OSL till att vara föremål för sekretess enligt 28 kap 11-12a OSL. Sekretess gäller då för uppgift om en enskilds personliga förhållanden om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men och uppgiften förekommer i ärende om arbetsförmedling. Om den arbetssökande gett sitt medgivande till att presenteras för en arbetsgivare får man anta att det ligger i den arbetssökandes intresse att detta sker snabbt, säkert och smidigt. Sekretess till skydd för en enskild hindrar inte att en uppgift lämnas till en annan enskild om den enskilde själv samtycker till det (10 kap 1 § och 12 kap OSL). Detta samtycke ska därmed ingå som en funktion och sparas så att det tydligt framgår att det finns ett samtycke och vad arbetssökanden har samtyckt till.

Vår bedömning är att, eftersom det är individen själv som för sina egna syften delar informationen genom elektronisk överföring, är reglerna om utlämnande av personuppgifter på ett medium för automatiserad behandling tillämplig enligt AF-PUF inte tillämpliga. Dataskyddsförordningens artikel 5 f och 32 är dock applicerbara så överföringen sker på ett säkert sätt i den nya funktionaliteten. För det fall att reglerna skulle anses vara tillämpliga finns stöd för utlämnande i 11 a § i Af-PUF. Där stadgas att personuppgifter som får behandlas enligt 3 § 1 och 6 AF-

PUF får lämnas ut på ett medium för automatiserad behandling till arbetsgivare. Rekryteringsföretagen får i detta avseende anses var ombud för arbetsgivare.

Observera att den tredje parten aldrig ska ha direktåtkomst till den enskildes information i det egna utrymmet. Om information ska delas ska det tydligt avskiljas för åtkomst (i någon form av utkorg) från all annan information som inte ska delas. Hämtningen av, eller delningen till tredje part ska alltid ske "logiskt avgränsat som en del av den totala säkerhetslösningen.

- Utforma användargränssnittet så att användaren måste acceptera användarvillkoren för e-tjänsten innan denna kan användas, exempelvis med en kryssruta.
- Utforma användargränssnittet med plats för tydlig och lättillgänglig information om Arbetsförmedlingens personuppgiftsbehandling i e-tjänsten (integritetsmeddelande).

5.4.11 Användarvillkor

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

Målsättningen med koncepttestet är att visa hur möjlighet till insyn och kontroll över data om individen hos offentlig, och i förlängningen, privat sektor kan ge tydliga mervärden för individen. Integritet och egen hämtning och delning har utgjort kärnan i framtagen PoC, och därmed också de juridiska förutsättningarna för att hantera och dela personliga data. PoC:en visar hur en individ kan hämta data från olika myndigheter och organisationer för att (hos AF) kunna skapa ett CV med validerade uppgifter/data från validerad källa (körkort, arbetsgivare, examens- och utbildningsdata, med mera) som sedan kan användas för att underlätta arbetssökande.

Levererad PoC är inte ett färdigt system som är klart att driftsätta. Framtagen PoC är att se som en utforskande testimplementation. Implementationen[80] är en CV-tjänst som integreras mot ett begränsat antal myndigheter och aktörer.

[80] Inom ramen för uppdraget har vi inte tagit fram en generell modell för säkerhets och integritetsfrågor, som t.ex hur en generell operator ska hantera & definiera vilka 3:e part tjänster som är pålitliga att dela data till.

6 Förvaltningsgemensam modell för insyn och kontroll

I detta kapitel beskriver vi hur ett så kallat individcentrerat dataekosystem, som ger individen ökad överblick, insyn och kontroll över de data om individen som finns hos offentlig sektor, kan utformas. Dataekosystemet beskrivs genom en förvaltningsgemensam modell som visar en önskad förflyttning där informationsdelningen utgår från individens behov och där denne är en aktiv part i informationsdelningen. Syftet är att information som redan finns hos offentliga aktörer ska kunna återanvändas i andra sammanhang.

Den förvaltningsgemensamma modellen är konceptuell vilket innebär att den nödvändiga förflyttningen skulle kräva att flera grundläggande förutsättningar tillkommer eller förändras. Det innebär att rättsliga, tekniska, semantiska och organisatoriska förutsättningarna för modellen behöver utredas vidare.

6.1 En konceptuell modell för individens insyn och kontroll

I regeringsuppdraget ingår bland annat att ta fram en eller flera lösningar som skulle kunna tillämpas förvaltningsgemensamt i svensk offentlig förvaltning för att individen med digitala verktyg ska få ökad insyn och kontroll över de data om individen som finns hos offentlig sektor.

Som en del av arbetet har vi därför tagit fram en konceptuell modell för att beskriva hur ett så kallat individcentrerat dataekosystem kan utformas för att ge individen ökad insyn och kontroll. Vi har sedan använt modellen i livshändelsen *bli sjukskriven* (avsnitt 6.2). Genom att använda den konceptuella modellen på livshändelsen illustrerar vi hur digitala verktyg för insyn och kontroll skulle kunna skapa nyttor för individen.

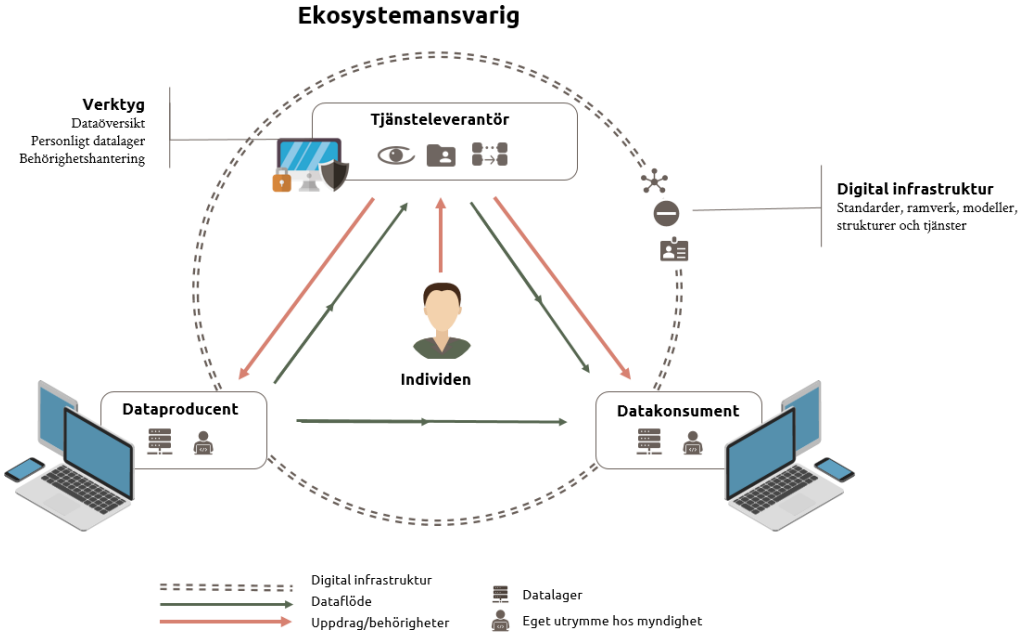
6.1.1 Ett individcentrerat dataekosystem

I syfte att hitta en, för den svenska förvaltningen, gemensam modell för att underlätta enskilda individers insyn och kontroll av uppgifter om sig själv som finns i den offentliga sektorn, och i förlängningen även uppgifter som finns i den privata sektorn, presenteras här en konceptuell modell av ett så kallat individcentrerat dataekosystem. Modellen har inspirerats delvis av konceptet med *Eget utrymme hos myndighet* men även av principerna bakom *MinaData* och *Solid* som beskrivits i avsnitten 6.1.3, 4.3.4 och 4.3.6.

Modellen är generisk, vilket innebär att den beskriver händelseförlopp på ett generellt och allmängiltigt sätt men modellen ska också kunna anpassas och tillämpas för specifika situationer och omständigheter. Modellen kan därmed

realiseras på olika sätt. Till exempel tillåter modellen individen att hämta data från en dataproducent för att sedan dela de med en datakonsument men också för att data delas direkt mellan en dataproducent och datakonsument utan mellanlagring. Figuren nedan visar den konceptuella modellen av det individcentrerade dataekosystemet.

Figur 5 Den konceptuella modellen av det individcentrerade dataekosystemet



En tanke med det individcentrerade dataekosystemet är att det är individen som, genom olika digitala verktyg, bestämmer när och hur data om individen ska delas med andra aktörer i dataekosystemet när informationsutbytet mellan aktörerna inte är reglerat i författning. Individen ska kunna via verktyget Dataöversikt se de uppgifter som individen är intresserad att ta del av. Därefter kan individen genom verktyget Behörighetshantering ge ett uppdrag (rosa pilar) till den dataproducent som har de aktuella uppgifterna i sitt datalager att lämna ut uppgifterna. Uppdraget innehåller även uppgifter om behörigheter vilket styr vem, förutom individen själv, som ska få ta del av uppgifterna.

6.1.2 Dataekosystemets uppbyggnad och dess aktörer

Bilden av dataekosystemet innehåller en digital infrastruktur som förvaltas av en ekosystemansvarig, därutöver finns tjänsteleverantörer, dataproducenter och datakonsumenter som anslutit sig till dataekosystemet samt enskilda individer. Olika aktörer antar olika roller beroende på situation.

- **Den digitala infrastrukturen** illustreras med en blå dubbelsträckad cirkel som förbinder de anslutna aktörerna. Infrastrukturen består av nödvändiga funktioner, standarder och ett regelverk för hur dessa ska tillämpas.
- **Ekosystemansvarig** är den aktör som ansvarar för och tillhandahåller den digitala infrastrukturen med nödvändiga funktioner till det individcentrerade dataekosystemet. Den digitala infrastrukturen och dess funktioner kan tillhandahållas av extern leverantör (som inte beskrivs i figuren). Ett exempel på en ekosystemsansvarig är DIGG för infrastrukturen för Digital post.
- **Tjänsteleverantör** är den aktör som anslutit sig till dataekosystemet genom att acceptera de tekniska och säkerhetsmässiga krav som den ekosystemansvarige uppställer. En tjänsteleverantör tillhandahåller en eller flera digitala verktyg för individens insyn och kontroll av data som finns hos dataproducenter och datakonsumenter. Kivra är ett exempel på en tjänsteleverantör som levererar en tjänst till invånarna som bygger på den digitala infrastrukturen för Digital post som DIGG ansvarar för och tillhandahåller.
- **Dataproducent** är en aktör som behandlar personuppgifter och som är ansluten till dataekosystemet. Dataproducentens verksamhet kan vara av offentlig eller privat karaktär, till exempel en myndighet eller vårdcentral. Dataproducenten genererar personuppgifter som lagras i ett datalager som används i dataproducentens verksamhet.
- **Datakonsument** är den som tar emot personuppgifter från en dataproducent på uppdrag av den individ som uppgifterna gäller, till exempel för att handlägga ett ärende på begäran av individen. Uppgifterna hamnar då vanligtvis i datakonsumentens datalager. Datakonsumenten är ansluten till dataekosystemet och kan vara av offentlig eller privat karaktär, till exempel en myndighet eller ett försäkringsbolag.
- **Individen** är en identifierbar fysisk person som genom digitala verktyg begär insyn i och kontroll över data om sig själv som finns hos dataproducenter eller andra aktörer i dataekosystemet.

6.1.3 Verktyg i dataekosystemet

För att skapa förutsättningar för individen att få insyn och kontroll över personuppgifter om sig själv behövs ett antal verktyg. Med verktyg avses sådana digitala funktioner som möjliggör och underlättar individens insyn och kontroll. I modellen finns verktygen behörighetshantering, dataöversikt och personligt datalager som tillhandahålls av tjänsteleverantörer. Tjänsteleverantörer kan erbjuda verktygen separat eller integrerade i en och samma digitala tjänst, till exempel i en mobilapplikation.

Dataöversikt är ett verktyg som ger individen insyn hos en eller flera dataproducenter och en visuell översikt över data om individen. Översikten kan till exempel visa vilka uppgifter som finns lagrade, den legala grunden för behandlingen och ändamålet för behandlingen av uppgifterna. Dataöversikten kan även innehålla information om hur länge lagring och behandling kommer att ske.

Personligt datalager är ett digitalt lagringsutrymme där endast individen har insyn i och kontroll över de uppgifter som lagras. Beroende på hur uppgifterna behandlas i det enskilda fallet kan ett personligt datalager vara ett verktyg som innebär att uppgifterna mellanlandar och lagras innan de delas med den avsedda datakonsumenten.

Eget utrymme hos myndighet är ett koncept som innebär att en myndighet tillhandahåller ett skyddat utrymme åt individen som kan bearbeta uppgifter och handling från myndigheten utan att myndigheten eller någon annan har tillgång till utrymmet. Uppgifterna och handlingarna i eget utrymme blir därför inte att betrakta som allmänna handlingar. Ett eget utrymme motsvarar i princip verktyget personligt datalager med den skillnaden att eget utrymme bara kan förekomma hos myndigheter.

Behörighetshantering är det verktyg som ger individen möjlighet att styra och villkora behörigheter för andra som ska få tillgång till uppgifterna om individen, till exempel vem som får se, bearbeta och lagra uppgifterna, hur länge uppgifterna får lagras samt för vilka ändamål de får behandlas.

6.1.4 Dataekosystemets digitala infrastruktur

Den digitala infrastrukturen består av nödvändiga funktioner, standarder och ett regelverk för hur dessa ska tillämpas. Infrastrukturen i det individcentrerade dataekosystemet bör i så stor utsträckning som möjligt utgöras av de olika

byggblock som växer fram inom ramen för den förvaltningsgemensamma infrastruktur som DIGG leder.

De byggblock som tas fram inom till exempel kategorin *Tillit och säkerhet* skulle kunna ligga till grund för att möta behoven av säkerhet inom dataekosystemet. Inom kategorin *Digitala tjänster* skulle byggblocken Mina ombud, Mina ärenden och Min profil var och en för sig eller tillsammans kunna skapa förutsättningar för den dataöversikt som behöver finnas inom ekosystemet. För dessa tre byggblock behöver ett standardiseringsarbete genomföras som kan utgöra ett ramverk med begreppsmodeller och regelverk för hur informationen ska tillgängliggöras. En förutsättning för hela modellen är att det finns tekniska regler och ramverk för hur det omfattande informationsutbytet ska gå till. Byggblocken API-hantering och indexering kan utgöra viktiga förutsättningar för informationsutbytet i ekosystemet.

6.1.5 Individens insyn enligt modellen

I det individcentrerade dataekosystemet har individen möjligheter att få en samlad bild över vilken typ av data (om individen) som finns lagrad hos olika dataproducenter. Genom verktyget *Dataöversikt* kan individen efterfråga om det finns data om honom eller henne hos någon dataproducent eller annan aktör som är ansluten till dataekosystemet.

Dataproducenter och andra som är anslutna till dataekosystemet ska svara på en sådan förfrågan från en individ i enlighet med de villkor som gäller för anslutning till dataekosystemet. Verktyget *Dataöversikt* skulle kunna bygga på s.k. indexering vilket innebär scanning av stora mängder data från olika dataproducenter i syfte att leta efter metadata om en viss individ. Den metadata som påträffas vid en sådan scanning innehåller tillräckliga uppgifter för att beskriva för individen hos vilken eller vilka dataproducenter som data finns, för vilka ändamål data samlats in, på vilken rättslig grund som data behandlas hos respektive dataproducent samt hur länge data kommer att lagras eller behandlas.

Verktyget *Dataöversikt* möjliggör således insyn över de data om individen som finns hos olika dataproducenter i ett individcentrerat dataekosystem. Dataproducenter kan, enligt den konceptuella modellen, vara aktörer från både offentlig och privat sektor, det vill säga såväl myndigheter som företag och organisationer.

6.1.6 Individens kontroll enligt modellen

Det individcentrerade dataekosystemet ska även ge individen möjligheter till kontroll över sådan data som finns lagrad hos olika dataproducenter genom olika verktyg. Verktyget *Behörighetshantering* ska ge individen möjlighet att styra och sätta villkor för andra som ska få tillgång till uppgifter om individen. Verktyget kan användas till exempel för att begära ut data, begära rättelse eller radering av data samt dela data från en dataproducenten till en datakonsument eller avsluta en sådan delning. Verktyget kan även ge individen möjlighet att peka ut från vilken källa en viss data ska hämtas.

Dataproducenter som är anslutna till dataekosystemet ska beakta individens begäran inom ramen för vad villkoren för anslutning till dataekosystemet anger. Dataproducenter ska även beakta individens begäran i förhållande till vad dataskydds- samt offentlighets- och sekretesslagstiftningen medger.

Individen kan, utöver att dela data direkt från en dataproducent till en datakonsument, dela data från dataproducenten via det digitala verktyget *Personligt datalager* till datakonsumenten. Flödet kan anpassas efter behov, det vill säga i enlighet med vad situationerna och omständigheterna kräver utifrån regleringen om informationssäkerhet, offentlighet och sekretess och dataskydd.

Om en myndighet erbjuder en digital tjänst för delning av data eller liknande, har myndigheten möjlighet att tillhandahålla tjänsten genom konceptet eget utrymme hos myndighet istället för via verktyget Personligt datalager.

6.2 Hur modellen kan underlätta en livshändelse

Följande utgår från livshändelsen att *bli sjukskriven* och använder den konceptuella modellen för att illustrera det mervärde som kan skapas för individen när denne får kontroll och insyn över data om sig själv. Målet är att förenkla kontakterna med och möjligheterna att lämna korrekta uppgifter till offentliga och privata aktörer för individen.

Vi utgår från en person som vi kallar Anna som blir sjuk en längre tid. Denna livshändelse gör att hon är i behov av att ta del av och vidarebefordra uppgifter som olika aktörer har om henne. Vi har delat upp att *bli sjukskriven* i tre steg:

1. Hon söker vård och får läkarintyg.
2. Hon ansöker om sjukpenning hos Försäkringskassan.
3. Hon söker ersättning från privat sjukförsäkring.

Annas behov av att kontakta, samt förmedla information till och mellan aktörerna, idag kommer nu att analyseras. Därefter, i avsnitt 6.2.2, presenterar vi ett hypotetiskt framtidsscenario. I scenariot visualiserar vi hur Anna får insyn och kontroll över relevanta data som hon behöver och som skulle underlätta i hennes kontakter med de olika aktörerna.

6.2.1 Nuläge

Anna söker vård och läkaren bedömer att Anna inte kan arbeta på grund av de symtom som hennes sjukdom ger. Läkaren utfärdar ett läkarintyg och frågar om Anna vill att intyget ska skickas elektroniskt direkt till Försäkringskassan. Eftersom Anna även behöver intyget för sin privata sjukförsäkring ber Anna också om en utskrift. Av 3 § patientlagen (2014:821) framgår att den som är skyldig att föra patientjournal ska på begäran av patienten utfärda intyg om vården. Läkaren frågar också Anna om hon godkänner sammanhållen journalföring, det vill säga att läkaren får se vad andra läkare har gjort för journalanteckningar i samband med hennes tidigare läkarbesök. Bestämmelser om sammanhållen journalföring finns i 6 kap. patientdatalagen (2008:355). Vårdcentralen är i detta fall att betrakta som en dataprocent och Försäkringskassan som en datakonsument.

Anna får ett sms från Försäkringskassan med information om att de fått ett läkarintyg och hon blir tillfrågad om hon vill ansöka om sjukpenning. Anna loggar in på Försäkringskassans e-tjänster och fyller i ansökan. För att ansökan ska bli komplett behöver Försäkringskassan ha vissa uppgifter om hennes anställning och inkomster som hon behöver söka rätt på. Innan Försäkringskassan kan göra utbetalningen till hennes bankkonto behöver Anna också uppdatera sina kontakt- och bankuppgifter.

Nära Anna efter tre månader ansöker om ersättning från sin privata sjukförsäkring behöver hon skicka med läkarintyget och beslutet om beviljad sjukpenning.

Sammanfattningsvis innebär nuläget att Anna har begränsade möjligheter att via digitala verktyg ha kontroll över vilka uppgifter som ska skickas mellan vårdgivare, Försäkringskassan och sitt privata försäkringsbolag.

Livshändelsen ställer också höga krav på Anna då hon behöver agera både projektledare och informationsbärare av relevant data om sig själv mellan olika aktörer och processen är långsam och administrativt tidskrävande. Hon har viss insyn, men inte överblick.

6.2.2 Hypotetiskt framtidsscenario

Detta avsnitt har till syfte att visa ett hypotetiskt framtidsscenario där individens uppgiftslämnande underlättas samtidigt som insynen i och kontrollen över data om individen ökar. För att denna hypotetiska framtidsbild ska kunna bli verklighet krävs att flera grundläggande förutsättningar tillkommer eller förändras.

I det följande visualiserar vi samma livshändelse ur ett hypotetiskt framtidsscenario. Vi använder den konceptuella modellen för att illustrera hur Anna får insyn och kontroll. De verktyg som är tänkta att ge Anna insyn och kontroll tillhandahålls av tjänsteleverantörer som beskrivs i avsnitt 5.1.2. Verktygen som ingår i den konceptuella modellen består av tre huvudsakliga komponenter (*behörighetshanteraren, personligt datalager samt dataöversikt*) som tjänsteleverantörer kan erbjuda separat eller integrerade i en och samma tjänst.

Målbilden är att:

- Anna genom digitala verktyg får insyn och kontroll.
- Anna får hjälp att göra rätt.
- Annas uppgiftslämnande underlättas.
- Anna och samhället sparar resurser.

Som stöd i sina kontakter med både myndigheter och företag samt för att hantera sin data använder Anna olika digitala verktyg.

I verktyget *Behörighetshanterare* har hon givit godkännande till myndigheter och offentliga organisationer att hämta hennes kontaktinformation och, när det är aktuellt med bankinformation. Därmed behöver Anna bara hålla sina uppgifter uppdaterade i tjänsten som tjänsteleverantören tillhandhåller. Myndigheter och andra organisationer kan då alltid få hennes aktuella uppgifter. Hon har också sedan tidigare genom behörighetshanteraren godkänt sammanhållen journalföring mellan sin vårdcentral och de specialistkliniker där hon får behandling för sin kroniska sjukdom. Innan besöket har läkaren tagit del av journaluppgifter från specialistkliniken för att bättre förstå de symtom hon beskrivit innan mötet och för att kunna göra en bättre medicinsk bedömning. Vårdcentralen är här datakonsument och specialistkliniken dataproducenten.

Figur 6 Datadelning i ett hypotetiskt framtidsscenario.

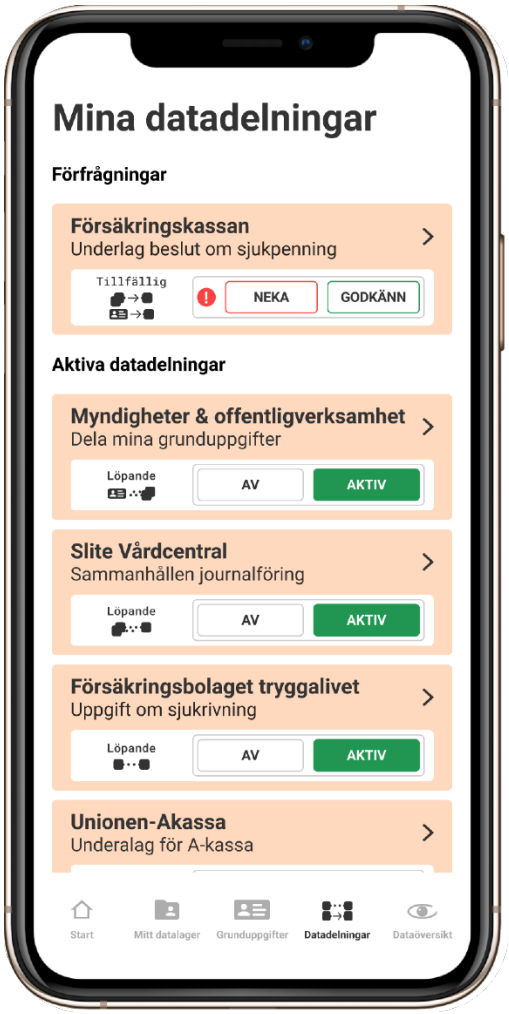
Läkaren undersöker Anna och bedömer att hon inte klarar sitt arbete på grund av sjukdomen och utfärdar därför ett läkarintyg. Anna vill att läkaren delar uppgifterna i läkarintyget direkt med Försäkringskassan. Läkaren på vårdcentralen är här dataproducent och Försäkringskassan datakonsument. Anna får en notis i den digitala tjänsten om att hennes läkarintyg nu finns i 1177:s intygstjänst. I tidslinjefunktionen ser hon att Försäkringskassan mottagit läkarintyget och Anna behöver inte oroa sig över om intyget kommit fram eller inte. Hon laddar också ned intyget till verktyget *Personligt datalager* i tjänsten.

Anna får en förfrågan från Försäkringskassan om hon har för avsikt att söka sjukpenning. Eftersom Anna vill söka sjukpenning klickar hon på länken till Mina sidor hos Försäkringskassan för att ansöka om sjukpenning.

För att Försäkringskassan ska kunna fatta beslut i hennes sjukpenningärende behöver Anna styrka sina inkomstuppgifter och sin tjänstgöringsgrad. Annas arbetsgivare har ett elektroniskt lönehanteringssystem där uppgifter om hennes tjänstgöringsgrad finns lagrade. Arbetsgivaren redovisar också kontinuerligt utbetalningar och skatteavdrag till Skatteverket digitalt.

Anna ser i *Behörighetshanteraren* för datadelning att Försäkringskassan vill ta del av dessa uppgifter. Hon ser i verktyget att ändamålet för uppgiftsinhämtningen är ”att fatta beslut om sjukpenning”. Anna ger via verktyget tillåtelse för Försäkringskassan att hämta uppgifterna en gång. Hennes arbetsgivare och Skatteverket är här dataproducenter och Försäkringskassan datakonsument.

Figur 7 Översikt av datadelning i ett hypotetiskt framtidsscenario



Anna har också en privat sjukförsäkring och har sedan tidigare godkänt att hennes försäkringsbolag automatiskt ska få information från Försäkringskassan när hon varit sjukskriven i tre månader. Hon får en förfrågan från försäkringsbolaget som behöver ta del av hennes läkarintyg och beslutet om sjukpenning för att handlägga hennes försäkringsärende. Försäkringskassan är nu dataproducent och hennes försäkringsbolag datakonsument.

Av integritetsskäl vill Anna inte att utomstående ska veta att hon söker ersättning från sitt privata försäkringsbolag. Hon har därför valt att uppgifterna först ska laddas ned till hennes personliga datalager som är ett verktyg där enbart Anna har insyn och där hon kan lagra uppgifter om sig själv. Därifrån delar hon läkarintyget med försäkringsbolaget.

Figur 8 Datadelning i ett hypotetiskt framtidsscenario

För Anna är det enkelt, snabbt och smidigt att dela relevanta uppgifter om sig själv som olika aktörer redan har om henne. Hennes uppgiftslämning underlättas också avsevärt av att verktygen stegvis leder henne genom processen och hjälper henne att göra rätt. Anna kan fokusera på sin rehabilitering och att återgå i arbete.

Den konceptuella modellen och den hypotetiska digitala tjänsten, och dess verktyg, skulle kunna ge Anna nödvändig överblick och insyn över:

- vilken typ av data som finns om henne,
- vilken organisation som har data om henne,
- för vilket ändamål uppgifterna samlats in (behandlas).

I detta framtidsscenario har Anna också kontroll genom att hon själv kan dela och avbryta delning av data om henne mellan olika aktörer. Anna kan också via verktyget ladda ned data i ett strukturerat och maskinläsbart format och dela den vidare till en annan aktör utan att den aktör som lämnade ut data vet vad hon ska använda dem till.

7 Rekommendationer till fortsatt utredning

Inom ramen för arbetet med detta regeringsuppdrag har vi identifierat att det finns stora värden i att ge invånarna ökad insyn och ökad kontroll över data om dem. Det har också blivit uppenbart att det finns flera olika sätt att tekniskt realisera en ordning som sätter individen i centrum och där individen kan ges överblick, insyn och kontroll.

Samtidigt som vi ser stor potential med ökad individcentrering när det gäller hur data hanteras ser vi också ett behov av att andra förutsättningar går i samma takt och riktning. Det har blivit tydligt att det finns en potentiell motsättning mellan å ena sidan den enskildes rätt till insyn och kontroll och å andra sidan myndigheters förutsättningar att realisera sådan insyn och kontroll. Därför lyfter vi fram följande rekommendationer för vidare arbete med frågan om ökad insyn och kontroll över personliga data.

7.1 Behovsundersökningar och analys

Det har inom ramen för detta regeringsuppdrag inte varit möjligt att genomföra undersökningar om behovet av insyn och kontroll hos befolkningen i Sverige eller hur det i så fall borde komma till utryck. Det behövs till exempel mer kunskap om individer vill ha mer sektorsvisa lösningar för insyn och kontroll eller om de föredrar helhetslösningar som spänner över sektorsgränserna. När data som spänner över stora områden, och med hög detaljeringsgrad, riskerar man att tappa överblicken som detta uppdrag syftar till att möjliggöra.

Vi anser därför att det bör undersökas hur användare av verktyg och tjänster för ökad insyn och kontroll vill att dessa ska utformas. Behoven hos individer behöver få en direkt påverkan på hur verktygen, bland annat dataöversikt, ska utformas och vilken funktionalitet som ska prioriteras. Undersökningen bör även resultera i en ökad förståelse för viktiga designaspekter av dessa verktyg. Detta kan ha en betydande inverkan på nyttjandegrad och är viktiga för en design som är digitalt inkluderande.

7.2 Utred specifika byggblocks påverkan på att möjliggöra ökad insyn och kontroll för individen

I den konceptuella modellen som presenteras i denna rapport ser vi att vissa av byggblocken som utvecklas eller håller på att tas fram inom den förvaltningsgemensamma digitala infrastrukturen skulle kunna skapa förutsättningar för individcentrerade ekosystem där individen har insyn och kontroll.

Byggblocken faller huvudsakligen inom kategorin *digitala tjänster* som omfattar byggblock som möjliggör standardiserad digital service från offentlig verksamhet för företag och invånare och *tillit* och *säkerhet* som omfattar byggblock som möjliggör standardiserade digitala funktioner för säkert informationsutbyte.

Vi föreslår att möjligheten att öka individens insyn och kontroll utreds vidare inom ramen för byggblocken Mina ombud, Mina ärenden och Min profil vilka skapar förutsättningar för den dataöversikt som vi anser behövs. Eftersom informationen i dessa byggblock troligtvis kommer ligga distribuerad hos källan, ser vi byggblocket Indexering som en viktig förutsättning för att möjliggöra ökad insyn eftersom denna mekanism pekar på var information om en aktuell individ finns.

7.3 Utreda möjligheten att främja insyn och kontroll utifrån eget utrymmet hos myndighet

Så kallat eget utrymme hos myndighet används redan idag av myndigheter för att ge service åt invånare och företag. Vid myndighetsgemensamma lösningar för egna utrymmen samt vid delning av information till och från egna utrymmen är dock rättsläget oklart. Vår samlade bedömning är att det med nuvarande ordning kan finnas utmaningar för myndigheter att realisera det individbaserade intresset av kontroll bland annat mot bakgrund av hur personuppgiftsansvaret är definierat i EU:s dataskyddsförordning, eftersom den potentiellt kan stå i konflikt med den möjlighet som myndigheter har att tillhandahålla tjänster genom ett eget utrymme utan att uppgifterna blir allmän handling. Den myndighet som tillhandahåller ett eget utrymme är personuppgiftsansvarig för den behandling som sker i utrymmet. Inom personuppgiftsansvaret ryms många skyldigheter i förhållande till de individer vars personuppgifter behandlas. Myndigheten ska inte ha någon egentlig rådighet över de uppgifter och handlingar som behandlas i ett eget utrymme för att det ska kunna betraktas som ett sådant utifrån regleringen i tryckfrihetsförordningen. Det behöver därför klargöras hur dessa två motstridiga intressen kan förenas i hållbara lösningar.

Uppgifter som behandlas i eget utrymme ska dessutom vara behövliga för myndighetens verksamhet. Det innebär att det utifrån ett dataskyddsperspektiv inte är möjligt att i ett eget utrymme hos en myndighet behandla uppgifter generellt utan koppling till myndighetens verksamhet. En sådan begränsning innebär att eget utrymme idag kan användas för att ge individen utökad kontroll, men då endast inom det verksamhetsområde som gäller för den aktuella myndigheten. Därmed blir det svårt att förverkliga idéer om helhet, översikt och kontroll.

Då flera relevanta rättsfrågor om eget utrymme idag får anses som olösta, rekommenderar vi att dessa utreds vidare. En viktig del i ett sådant arbete är att undersöka de rättsliga förutsättningarna och begränsningarna avseende personuppgiftsansvarets räckvidd i förhållande till eget utrymme. En annan viktig del är att utreda hur eget utrymme kan utformas i syfte stödja en individcentrerad datadelning inom sektorer eller livshändelser. Detta arbete kan med fördel göras i samråd med Integritetsskyddsmyndigheten i syfte att åstadkomma ett proaktivt förhållningssätt och i ett tidigare skede uppmärksamma behov av att anpassa regelverk.

7.4 Utveckla myndigheters serviceskyldighet

Serviceskyldigheten enligt 6 § förvaltningslagen utgör inte en rättslig grund för den behandling av personuppgifter som aktualiseras i den konceptuella modellen eller livshändelserna. Att dela uppgifter med andra myndigheter och enskilda, även om det skulle vara på uppdrag av individen, ingår således inte i serviceskyldigheten. Detsamma gäller för eventuellt informationsutbyte mellan myndigheter och privata aktörer. Idag regleras myndigheters behandling av personuppgifter genom sektorspecifik lagstiftning. Den rättsliga statusen för digitala informationsöverföringar och möjligheter att ge individen insyn och kontroll får anses som osäker.

Om serviceskyldigheten däremot omfattade utlämnanden och informationsöverföring till individen och andra myndigheter på digitala medier skulle myndigheterna ha större möjligheter att tillgodose den enskildes insyn och kontroll. Som exempel skulle en sådan serviceskyldighet kunna underlätta förvaltningsgemensamma lösningar gällande insyn och kontroll som baseras på egna utrymmen och digitala informationsöverföringar mellan myndigheter.

Vi föreslår att en konsekvensanalys av en utvidgning av serviceskyldigheten genomförs tillsammans med en av den särskilda dataskyddsregleringen (registerlagar) och möjligheten att lämna ut uppgifter i elektronisk form.