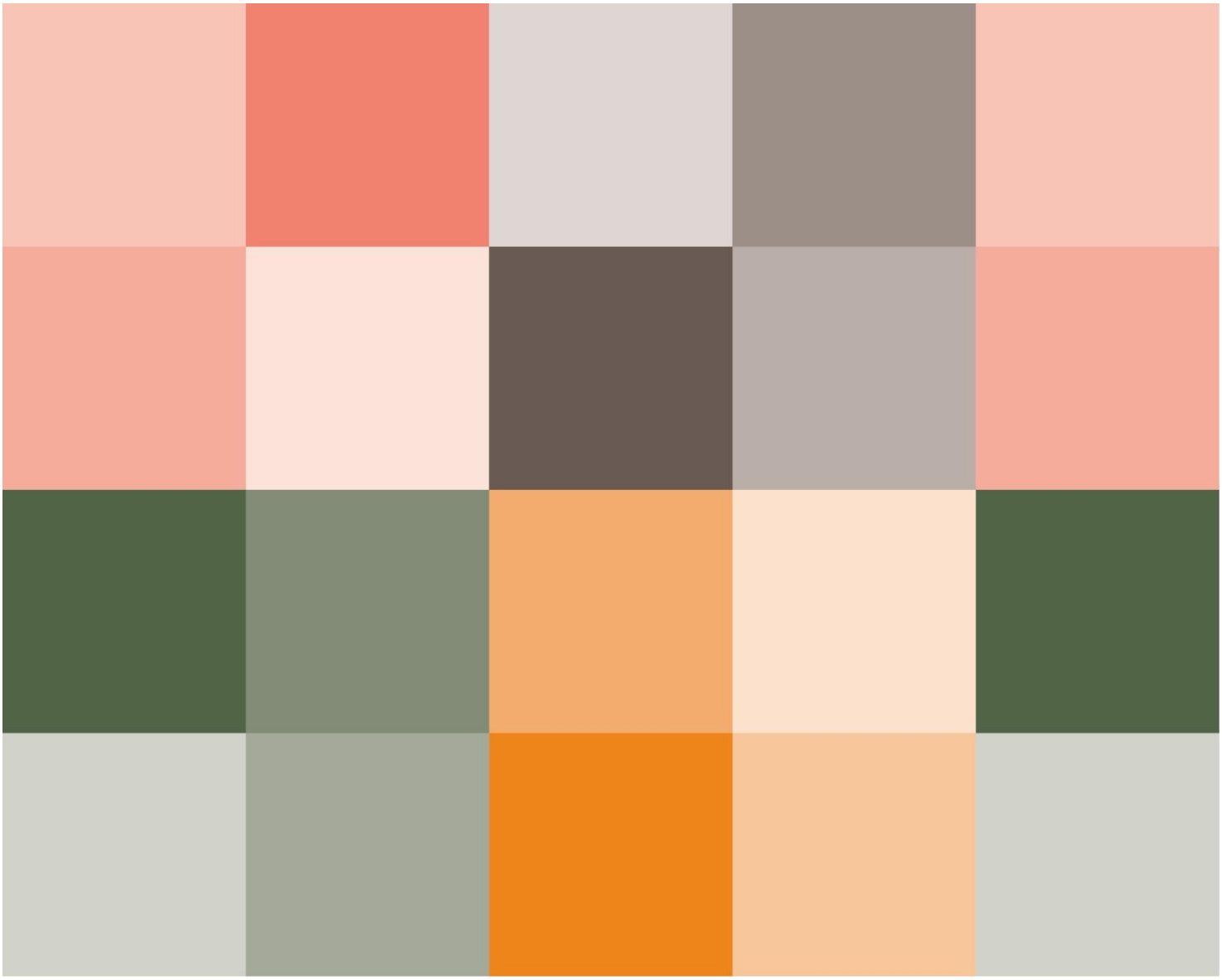


Bilaga 2

Omvärldsanalys (från uppdrag att möjliggöra lösningar för individen till kontroll och insyn av data om individen)

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Innehållsförteckning

1.1 Genomförande

Omvärldsanalysen genomfördes utifrån tematiserad bevakning och analys där varje deltagande myndighet bidrog med sin expertis och kompetens inom utvalda analytiska parametrar. Efter initiala jämförelser av olika nationella initiativ som på ett eller annat sätt bidragit till ökad insyn och/eller kontroll för individen i relation till hanteringen av data om individen hos offentlig aktör så blev det tydligt att det inte finns heltäckande lösningar i omvärlden som Sverige kan kopiera och implementera. Unika nationella förhållanden, kulturella och institutionella såväl som lag- och regelmässiga gör att Sverige bör först etablera en medborgarförankrad vision för hur man vill se hanteringen av personliga data och i vilket syfte det vill säga vad man förväntar sig att vinningen blir, för individer, myndigheter, näringsliv och samhället i stort.

Därefter är det i stor grad en fråga om man vill se ett ekosystem för delning av data inom vilken majoriteten av delningar kan ske med individens rätt till insyn och kontroll i centrum för arkitekturen, och där offentliga och privata aktörer kan anta olika roller och ansvar beroende på i vilket skede av en händelse en specifik datatransaktion initieras. Möjligen är ett mer fragmenterat system med olika lösningar för olika händelser mer eftertraktat så länge som de olika systemen är kompatibla med varandra. Det som är den stora frågan är om man vill se över och göra ändringar i lagstödet för delningar av data mellan olika typer av aktörer och nyttja den befintliga expertisen inom arkitektur att bygga ett mer omfattande system eller om man vill undvika juridiska komplikationer i högsta möjliga mån och således bygga enskilda lösningar för specifika fall som är mer begränsade men som kan effektivisera vissa delar av ett händelseförlopp samt ge individen ökad insyn och kontroll i just dessa skeden.

För att utvärdera denna fråga genomfördes flertalet erfarenhetsöverföringsmöten under den inledande perioden av uppdraget med bland flera eSam om deras tidigare arbete med MinaData principerna och förberedande arbete med projektet Mitt Digital Hem, med JobTech och användarfall som involverat delning av data mellan myndighet och privat aktör samt eHälsomyndigheten och projektet Hälsa för Mig. De samlade intrycken och lärdomarna beskrivs i detta kapitel men för en mer detaljerad genomgång av omvärldsanalysens medtag från granskningen av EU, FN och OECD samt olika länders nationella initiativ, vänligen se *bilaga D*.

1.2 Europeiska Unionens ställningstagande gentemot insyn och kontroll

För att säkerställa en väl fungerande inre marknad och uppnå väl avvägda tjänster och möjligheter för EU-medborgare, både avseende användbarhet och säkerhet, har flertalet lagar och förordningar beslutats inom EU de senaste åren med bäring på frågan om att ge individen ökad insyn och kontroll över data om personen.

1.2.1 Single Digital Gateway

Single Digital Gateway-förordningen (SDG) innebär tillhandahållandet av 20 gränsöverskridande e-förvaltningstjänster som kräver att den offentliga förvaltningen återanvänder data som medborgare och företag redan har tillhandahållit. För att uppnå detta krävs standardisering av datamängder, semantik och en infrastruktur för gränsöverskridande datautbyte i realtid.

En av de bärande principerna för att SDG-förordningen ska kunna fungera bygger på The Once Only Principle (TOOP) vilken innebär att medborgare och företag endast behöver lämna uppgifter en gång i kontakt med offentliga förvaltningar. Offentliga förvaltningsorgan vidtar åtgärder för att internt dela och återanvända dessa uppgifter, även över EUs gränser och alltid med hänsyn tagen till dataskyddsföreskrifter och andra regulatoriska begränsningar.

TOOP-konceptet fokuserar på att minska den administrativa bördan för individer och företag genom att omorganisera den offentliga sektorns interna processer, istället för att medborgare och användare anpassar sig till befintliga rutiner.

Dessutom har europeisk lagstiftning också fokuserat på informations- och cybersäkerhet vilket påverkar möjligheterna till insyn och kontroll för medborgare och företag. Enligt lagstiftningen (GDPR) och direktivet (nätverks- och informationssäkerhetsdirektivet) som gäller General Data Protection Regulation NIS för leverantörer av tjänster och digitala plattformar, måste säkerhetskrav införas och användare eller tillsynsmyndigheter meddelas om incidenter inträffar. GDPR ställer också höga krav kring hanterandet av personliga data både vad gäller insamlande, processande men också gällande lagring och gallring.

1.2.2 E-ID-tjänsteförordningen (eIDAS)

E-ID-tjänsteförordningen (eIDAS) innebär möjligheter till elektronisk identifiering av fysiska och juridiska personer och regler för betrodda tjänster, i synnerhet för elektroniska transaktioner. eIDAS är en förutsättning för att SDG-

förordningen och TOOP-konceptet ska kunna fungera på ett tillfredsställande sätt och för att tillitsnivån till erbjudna tjänster ska kunna garanteras.

1.2.3 EU-cybersäkerhetslagen

Den nya EU-cybersäkerhetslagen skapar en ram för EU-certifiering som innebär att länder frivilligt kan instifta bestämmelser om att företag måste certifiera informations- och kommunikationsteknikprocesser, -produkter och -tjänster för att skapa förtroende hos användarna. Företag kan till exempel certifiera produkter som uppkopplade bilar och smarta medicintekniska produkter.

1.2.4 EU:s Datastrategi

EU-strategin för data[1] är en strategi för politiska åtgärder och investeringar i dataekonomin under de kommande fem åren. Slutmålet för EU är att dra nytta av fördelarna med bättre dataanvändning, vilket kan vara; ökad produktivitet, förbättringar inom hälsa och välbefinnande, miljö, transparent styrning och bekväma offentliga tjänster. Skapandet av ett gemensamt europeiskt dataområde innefattar en genuin inre marknad för data som är öppen för data från hela världen, där både personuppgifter och icke-personuppgifter, inklusive känsliga företagsuppgifter, är säkra och företagen ändå lätt kan få åtkomst till en närapå oändlig mängd industriella data av hög kvalitet samt främjandet av tillväxt och värdeskapande som samtidigt minimerar människans koldioxidavtryck och miljöavtryck.

Unionens strikta dataskyddsregler anses vara ett instrument för att säkra allmänhetens tillit till kommande datadrivna innovationer och delning av personuppgifter inom EU. I Förenta staterna överlåts organiseringen av dataområdet åt den privata sektorn, med betydande koncentrationseffekter och Kina har en kombination av statlig övervakning och teknikjättar utan tillräckliga garantier för enskilda personer. EU:s potential kan enbart realiseras om hög integritet, säkerhet och etiska standarder genomsyrar utvecklingen, annars kommer konkurrenternas alternativ att även fortsatt dominera den europeiska marknaden.

[1] 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

Ett gemensamt europeiskt dataområde och en genuin inre marknad för data är beroende av en gemensamt hållen vision mellan medlemsländerna. Gemensamma framsteg måste göras på en rad områden så som till exempel tillgång till data. Infrastrukturen bör stödja skapandet av europeiska datapooler som möjliggör stordataanalys och maskininlärning.

1.2.4.1 Tillgängliggörande av data

På en övergripande nivå behövs data tillgängliggöras för att samhälls-, klimat- och miljöutmaningar ska kunna tas itu med och mer hållbara samhällen skapas. Brist på rättslig klarhet om vem som kan göra vad med data (framför allt data från sakernas internet) hindrar datadelning mellan företag och ett EU-regelverk för offentliga sektorns vidareutnyttjande i allmänhetens intresse av data som innehas av privata aktörer utred för att även öka delningen av data mellan privata och offentliga aktörer.

Delning mellan myndigheter kan i sin tur, i hög grad bidra till att förbättra beslutsfattandet och offentliga tjänster men även till att minska den administrativa bördan för företag som är verksamma på den inre marknaden. Dessutom finns ett ansvar att förbättra den offentliga sektorns egna förmåga att utnyttja data för beslutsfattande och erbjuda offentliga tjänster. Incitament till organisationer som bidrar med data rekommenderas i form av till exempel ökad tillgång till data från andra bidragsgivare, analysresultat från datapooler, eller tjänster såsom prediktivt underhåll.

I nuläget finns inte tillräckligt med data tillgängliga för utveckling av artificiell intelligens eller skapandet av mer innovativa offentliga tjänster. Information som innehas av myndigheter har producerats med offentliga medel och bör därför vara till nytta för samhället och bör tillgängliggöras genom till exempel förmånstillgång, till forskare, andra offentliga institutioner, små och medelstora företag eller uppstartsföretag. Användningen av aggregerade och anonymiserade data från den privata sektorn kan också vara värdefulla som en kollektiv nyttighet och bidra till det allmännas bästa.

Direktivet om öppna data[2] säkerställer att den offentliga sektorn gör en större mängd av de data den producerar enkla att tillgå och använda och exempel på

[2] Direktiv (EU) 2019/1024

nyttjande finns samlade på den europeiska portalen för öppna data.[3] Men problem kvarstår med att dataset av högt värde ofta inte är tillgängliga på samma villkor i hela EU.

Det finns även betydande interoperabilitetsproblem som gör det omöjligt att kombinera data från olika källor inom samma sektor eller mellan sektorer. Den löpande planen för IKT-standardisering och en förstärkt europeisk interoperabilitetsram för offentliga tjänster syftar till att insamling och behandling av data från olika källor sker på ett enhetligt och interoperabelt sätt.[4] [5]

1.2.4.2 Förordningar, direktiv och lagstiftning

Ändamålsenlig lagstiftning och styrning behövs för att säkerställa tillgången till data genom riktade investeringar i standarder, verktyg och infrastrukturer samt kompetens att hantera data. EU:s förmåga att investera i nästa generations teknik och infrastruktur samt i digitala färdigheter kommer vara avgörande för att säkra EU:s tekniska suveränitet. Den allmänna principen ska vara att underlätta frivillig datadelning med ett förtydligande av reglerna för ansvarsfull användning och delning av data.

EU-kommissionen listar flera initiativ som har främjat utvecklingen av dataekonomin såsom:

- förordningen om det fria flödet av andra data än personuppgifter (förordning (EU) 2018/1807)
- cybersäkerhetsakten (förordning (EU) 2019/881)
- direktivet om öppna data (direktiv (EU) 2019/1024)
- direktivet om digitalt innehåll (direktiv (EU) 2019/770)

Den kommande översynen av den allmänna dataskyddsförordningen anses kunna resultera i ytterligare åtgärder för att stärka tilliten i europeisk användning av data och komplettera ovan initiativ.

Flera medlemsstater har börjat anpassa sina rättsliga ramar exempelvis en fransk lag som ger den offentliga sektorn rätt att få åtkomst till vissa data av allmänt

---

[3] https://www.europeandataportal.eu/en/using-data/use-cases

[4] https://ec.europa.eu/digital-single-market/en/news/rolling-plan-ict-standardisation.

[5] https://ec.europa.eu/isa2/eif_en. Se COM(2017) 134 final.

intresse från den privata sektorn[6] och en finsk lag om sekundär användning av personuppgifter inom social- och hälsovården, genom vilken en tillståndsmyndighet inrättas.[7] EU-lagstiftningen får inte äventyras av rättsliga anspråk från länder utanför unionen. Genom sektorsöversyner bör man kartlägga rättsliga och andra hinder för användningen av data och databaserade utbud. Standardisering av data möjliggör gränsöverskridande efterlevnad i realtid och bör således leda till minskade administrativa bördor och hinder på den inre marknaden.

Europeisk molninfrastruktur och molntjänster dras med problem i fråga om både utbud och efterfrågan vilket gör offentliga aktörer beroende av externa leverantörer och sårbara för externa hot. För molnbaserade tjänster är tjänsteleverantörer verksamma i EU även ofta omfattade av tredjeländers lagstiftning vilket innebär att data kan bli åtkomliga för tredjeländers jurisdiktioner som inte följer EU:s dataskyddsram. Den amerikanska CLOUD-lagen väcker till exempel legitima farhågor för EU:s företag, medborgare och myndigheter när det gäller tillämplig av europeiska dataskyddsregler. Under 2022 kommer kommissionen ge ut en regelbok för molntjänster vilken kommer utgöra ett kompendium av befintliga uppförandekoder och certifieringar avseende säkerhet, energieffektivitet, tjänstekvalitet, dataskydd och dataportabilitet. Kommissionen kommer även jobba för att underlätta utvecklingen av gemensamma EU-standarder och krav för offentlig upphandling av databehandlingstjänster (möjligen kommer man efterlikna det amerikanska offentliga upphandlingsprogrammet FedRAMP[8]).

Inom offentlig sektor har förhållandevist få börjat använda molnteknik vilket lett till att kostnader inte minskat och inga nya resurser frigjort för ytterligare effektivisering inom offentlig förvaltning. Myndigheter bör främja efterfrågan genom ökad användning av dataanalys och automatisering i offentliga tjänster och offentligt beslutsfattande.

---

[6] LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique
[7] 552/2019
[8] https://www.fedramp.gov/

Föreslagna lagstiftningsåtgärder bygger på fyra pelare:

1. *En sektorsövergripande styrningsram för tillgång till och användning av data.*

Förhoppningarna är att ramen ska gynna experimenterande till exempel regulatoriska sandlådor, iteration och differentiering. Man vill även underlätta gränsöverskridande användning av data och tydliggöra vilka data som kan användas i vilka situationer vilket är av särskild betydelse för känsliga data som inte omfattas av direktivet om öppna data. Antagandet av en genomförandeakt om dataset med högt värde ska öppna upp centrala referensdata från den offentliga sektorn för innovation och göra dessa dataset tillgängliga kostnadsfritt i hela EU, i ett maskinläsbart format och genom standardiserade programmeringsgränssnitt.

En annan prioritet är krav och standarder för interoperabilitet inom och mellan sektorer vilket uppmanades till i ministerförklaringen om e-förvaltning (Tallin Deklarationen) 2017.[9] Detta kan göras i enlighet med principerna om uppgifternas sökbarhet, tillgänglighet, kompatibilitet och återanvändbarhet (Fair) med beaktande av de sektorspecifika myndigheternas utveckling och beslut.[10]

EU:s portal för öppna data ska vara ett exempel på hur man bör organisera sina egna data, använda dem för bättre beslutsfattande och göra de data man producerar och finansierar tillgängliga för andra.[11] Principen för tillgängliggörandet av data från till exempel forskning är *så öppen som möjligt, så begränsad som nödvändigt*" vilket ska exemplifieras av det europeiska öppna forskningsmolnet.[12]

2. *Investeringar i data och stärkande av EU:s kapacitet och infrastruktur för att hysa, behandla och använda data samt interoperabilitet*

Utöver fastställande av standarder, utveckling av verktyg, insamling av bästa praxis för hantering av personuppgifter krävs även investeringar från både den privata och den offentliga sektorn för utbyggnad av nästa generations infrastruktur för databehandling. Investeringar kommer att samordnas med relevanta myndigheter i medlemsstaterna och med investeringar genom struktur-

[9] Tallinn Declaration on eGovernment at the ministerial meeting during Estonian Presidency of the Council of the EU on 6 October 2017 sid. 4

[10] Fairdataprinciperna: https://www.force11.org/group/fairgroup/fairprinciples

[11] https://data.europa.eu/euodp/en/data/

[12] https://ec.europa.eu/research/openscience/index.cfm?pg=open-science-cloud

och investeringsfonderna. Under perioden 2021–2027 kommer infrastruktur, datadelningsverktyg, arkitektur och styrmekanismer för livskraftiga ekosystem för datadelning och artificiell intelligens finansieras.

3. *Ge enskilda personer mer inflytande, investera i kompetens och i små och medelstora företag*

Att ge användarna inflytande över sina egna data och möjlighet att kunna hävda sina rättigheter när det gäller användningen av de data de genererar är enhetligt med den allmänna dataskyddsförordningen. De kan ges inflytande över sina data genom verktyg och metoder för att på detaljnivå besluta om vad som görs med uppgifterna (”personliga dataområden”). Enskilda personers rätt till dataportabilitet stöds av artikel 20 i den allmänna dataskyddsförordningen[13] och skulle ge individen mer kontroll över vem som kan få åtkomst till och använda maskingenererade data. 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.

MinaData rörelsen som förespråkar åtgärder och verktyg som skulle kunna ge enskilda personer möjligheten att på detaljnivå kunna besluta vad som görs med deras data, anses kunna ge betydande fördelar för enskilda personer såsom bättre personliga finanser, minskad miljöpåverkan, underlättad tillgång till offentliga och privata tjänster, bättre hälsotillstånd samt ökad tillsyn och insyn gällande personuppgifter. Enligt data strategin måste sådana verktyg 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.*[14] EU-kommissionen anser att sådana verktyg har en betydande potential och behöver en stödjande miljö.

Decentraliserad digital teknik som blockkedjeteknik ger ytterligare möjligheter för både privatpersoner och företag att hantera dataflöden och användning av data, på grundval av fritt val och självbestämmande. I kombination med olika typer av

[13] https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/dataskyddsforordningen---fulltext/#20

[14] 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

kompensationsmodeller anser man att dynamisk dataportabilitet i realtid incitamenteras och blir möjlig för både enskilda och företag.

Dataaltruism är ett begrepp som används för att beskriva den enskildes vilja att tillåta att de data hen genererar, används för det allmännas bästa i överensstämmelse med den allmänna dataskyddsförordningen. Personer som vill dela sin data i detta syfte, till exempel för forskningssyften, borde ha ökad möjlighet att bestämma detta själva och aktivt dela den. Utöver frivillig delning bör dataåtkomsträttigheter vara sektorsspecifika och ges endast med hänsyn till datainnehavarens legitima intressen och respektera den rättsliga ramen.

4. Gemensamma europeiska dataområden inom strategiska sektorer och domäner av allmänt intresse

Med strategiska menas områden där användningen av data kommer att få systemeffekter på hela ekosystemet och även på medborgarna. Med utgångspunkt i pågående arbete med det europeiska öppna forskningsmolnet kommer kommissionen att stödja inrättandet av följande nio gemensamma europeiska dataområden:

- Ett gemensamt europeiskt dataområde för tillverkningsindustrin
- Ett gemensamt europeiskt dataområde för gröna näringar
- Ett gemensamt europeiskt dataområde för rörlighet
- Ett gemensamt europeiskt dataområde för hälsa
- Ett gemensamt europeiskt dataområde för finans
- Ett gemensamt europeiskt dataområde för energi
- Ett gemensamt europeiskt dataområde för jordbruk
- Gemensamma europeiska dataområden för offentlig förvaltning
- Ett gemensamt europeiskt dataområde för kompetens

Åtgärderna för dataområdet för offentlig förvaltning inriktas på juridiska data och data från offentlig upphandling samt andra områden av allmänt intresse såsom användning av data för att förbättra brottsbekämpningen i EU i enlighet med EU-rätten, bland annat proportionalitetsprincipen och dataskyddsreglerna. Området är även en möjliggörare för innovativa ”govtech”-, ”regtech”- och ”legaltech” tillämpningar.

1.3 Förenta Nationerna

1.3.1 ID som mänsklig rättighet

I artikel 6 av den allmänna förklaringen om de mänskliga rättigheterna står det att v*ar och en har rätt att överallt erkännas som en person i lagens mening.*[15] 70 år efter att förklaringen publicerades har FN antagit en *mänsklig rättighetsbaserad strategi för data* som kallas HRBAD (A Human Rights-Based Approach to Data) vilken fokuserar på frågor om datainsamling och uppdelning. HRBAD, i enighet med Agenda 2030 för hållbar utveckling och i linje med de globala hållbarhetsmålen (specifikt mål 16.9 som syftar till att *tillhandahålla juridisk identitet till alla, inklusive födelseregistrering, senast 2030*) hjälper 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.[16]

Preliminära principer, rekommendationer och god praxis har formulerats under rubrikerna:

- Deltagande (Participation)
- Uppdelning av data (Data disaggregation)
- Självidentifiering (Self-identification)
- Transparens (Transparency)
- Integritet (Privacy)
- Ansvarighet (Accountability)

Deltagande är en central princip som bör gälla hela datainsamlingsprocessen från strategisk planering och metodval till identifiering av behov och analys av data. Uppdelade data behövs för att kunna samla in mer detaljerade data om individen som möjliggör identifiering och mätning av ojämlikheter mellan populationsgrupper snarare än att beslutsfattande endast baseras på nationella genomsnitt. Individer borde dock kunna välja fritt om de vill dela information om deras personliga attribut eftersom den typen av data, speciellt detaljerade data insamlad från marginaliserade grupper, kan användas för ondo. Kategorisering av

[15] https://www.regeringen.se/contentassets/d6d5653029e14e338a4b86f5f4b34c6b/fns-konventioner-om-manskliga-rattigheter

[16] https://www.ohchr.org/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf

populationsgrupper borde ske med deltagande från individer eftersom kategoriseringen endast kan göras korrekt utifrån individens självuppfattade grupptillhörighet.

Om man lyckas säkra deltagande i undersökningar så att de är representativa för hela befolkningar och innehåller information som kan nyttjas för värdeskapande jämförelser inom och mellan grupper där individerna dessutom har haft möjlighet att själva identifiera sin grupptillhörighet så har man kommit en bra bit på vägen. Sedan behöver man säkra att de rättsliga, institutionella och politiska ramarna enligt vilka nationella chefstatistiker och statistiska system fungerar är offentligt tillgängliga för att skapa förtroende för den statistiska information som producerats.

1.3.2 ID2020 – Ett digitalt universal ID

På FN:s toppmöte ID2020 samlades privata företag såsom Microsoft och Accenture och humanitära grupper inklusive World Food Programme och FN:s flyktingbyrå med ett gemensamt mål om att skapa digital identifiering för varje person på planeten som är kopplad till fingeravtryck, födelsedatum, hälsojournaler, utbildning, resor, bankkonton och mera.[17]

Ett digitalt universal ID kan vara en bekvämlighet för många men en överlevnadsfråga för andra, speciellt flyktingar där avsaknaden av medtagen dokumentation inte bara är ett problem under själva flykten utan även under en eventuell period av integrering i ett nytt samhälle. Toppmötet hade ett större focus på att visa på möjliga framtida lösningar än att bygga konsensus kring en specifik lösning. Accenture demonstrerade en prototyp i form av en app som bland annat använder QR-koder för att identifiera individer.[18] Farhågor om att samla så mycket information om en individ på en plats anses kunna komma att hanteras med lösningar baserade på blockkedjeteknologi.

På ID2020 mötet India lyfts som exempel på hur ett samhälle med en digital ID-lösning av denna sort kan se ut. 2009 lanserades Aadhaar[19], ett digital ID program där medborgare frivilligt kan lista namn, födelsedatum, kön, adress,

[17] https://id2020.org/digital-identity

[18] https://youtu.be/QYy8a7HDJ0g

[19] https://uidai.gov.in/what-is-aadhaar.html

telefonnummer, tio fingeravtryck och två ögonskanningar samt foto. I utbyte kan användare nyttja den digitala ID:n för att signera dokument online, ansöka om kredit och om jobb, identifiera sig på sjukhus och skicka pengar med mera. 25 miljoner autentiseringar görs dagligen med Aadhaar som i juni 2020 nådde 1,1 miljarder användare (cirka 85 % av befolkningen). Samtidigt visar exemplet med Indien även upp problem då information om 130 miljoner människor befaras ha läckt från fyra olika statliga websidor. En av lösningarna som diskuteras är att ge ägandeskap och kontroll av personliga data till användaren via *arkitektur för elektroniskt samtycke*.

2018 skapades ID2020 alliansens manifest[20] i samarbete med FN: s flyktingkommissarie (UNHCR) med etiska överväganden kring digital identitet. Där man likställer förmågan att kunna bevisa sin identitet med en grundläggande och universell mänsklig rättighet. Man anser att det borde finnas ett komplement till traditionella nationella identitetshandlingar som inte är beroende av styrande regimers anseenden om eller behandling av grupperingar inom nationalstater. För många icke-erkända minoriteter, flyktingar och individer marginaliserade av andra anledningar behövs en identitetshandling som inte är kopplad till en nationalitet. Individer borde ha kontroll över sina egna digitala identiteter och över hur data kring deras identitet samlas in, används och delas. Integritetsskydd och portabilitet behövs för at ten digital identitet ska stärka och skydda individer på ett meningsfullt sätt.

Kryptografiskt säkra, decentraliserade system och andra tekniska lösningar ökar möjligheterna för säkra digitala identiteter men det behövs bred konsensus om styrande principer, designmönster, interoperabilitetsstandarder och andra policy ramverk för att decentraliserade digitala identiteter ska erkännas och vara betrodda.

Kärnkraven på en digital identitet som uppfyller kraven och visionen som ID2020 alliansen satt fram representeras av de fyra P:na:

- Privat (private) – endast användaren kontrollerar sin egna identitet, vilka data som delas och med vilka

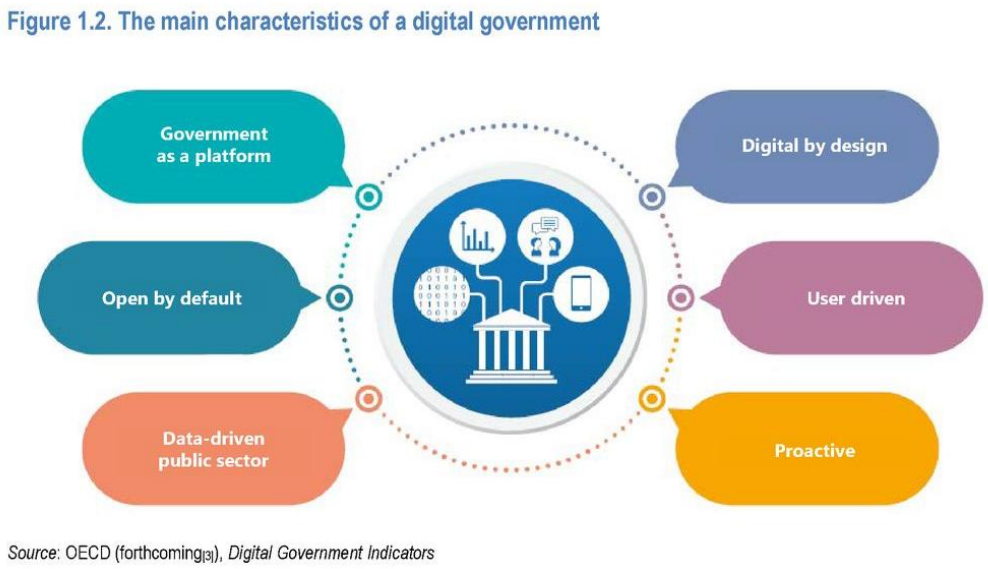
[20] https://id2020.org/manifesto

- Portabel (portable) – identitetsstärkande information är tillgänglig var än användaren befinner sig och på olika sätt
- Beständig (persistent) – din digitala identitet följer dig från födsel till döden
- Personlig (personal) – Identiteten är unik för användaren

1.4 OECD

Det finns inga eller få mätningar som jämför hur länders framsteg på området digital identitet eller mekanismer för att stärka individens ställning genom ökad insyn och kontroll för individen över personliga data. Det finns dock nya indikatorer under utveckling som till exempel indikatorer för digitala myndigheter som kan vara av intresse för att utvärdera hurvida förmågor utvecklas för att kunna erbjuda tjänster utifrån ett ekosystem som möjliggör för samverkan mellan individer, näringsliv, offentlig förvaltning och civilsamhället.

Figur 1 Huvudegenskaper av digital förvaltning



1.4.1 Public Governance Policy Papers - Digital Government Index (DGI) 2019

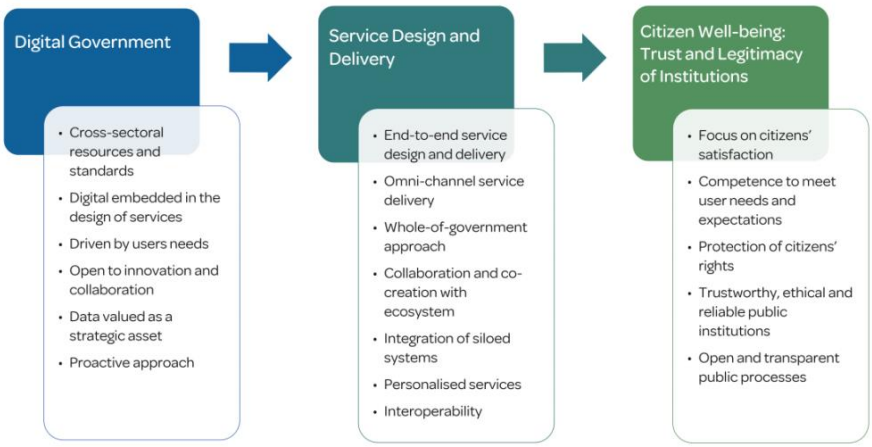
Vad säger OECD:s DGI om hur länder ökar medborgares möjligheter till ökad insyn och kontroll över sina personliga data? Utvärderingen baseras på hur olika länder presterat utifrån sex olika dimensioner som en helt digital regering uppvisar. Dessa är:

1. Digital via design (digital by design)
2. Regering som plattform (government as a platform)
3. Datadriven offentlig sektor (data-driven public sector)
4. Öppen som standard (open by default)
5. Användardriven (user-driven)
6. Proaktivitet (proactiveness)

Korea, Storbritannien, Columbia, Japan och Danmark pekas ut som de länder som lyckats bäst med att prestera inom alla sex dimensioner vilket visar på ett helhetstänk i deras respektive digitaliseringsstrategier. Bland rapportens slutsatser och rekommendationer återfinns 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. Man uppmuntrar visserligen till proaktiv styrning utifrån att data gjorts tillgänglig och återanvänts inom och utanför den offentliga sfären för att skapa värde och främja medborgarnas välbefinnande men man nämner inte möjligheten för den enskilde att styra över sin datas användning och delning som en del av denna policy.

Inte heller under rubriken för medborgares välbefinnande finns ökad insyn och kontroll för den enskilde med om man utgår ifrån att en öppen och transparent offentlig sektor inte per definition betyder ökad insyn i personliga data såsom detta definieras inom detta uppdrag.

Figur 2 Vägen mot ökat välmående hos medborgare



I utvärderingen av dimensionen datadriven offentlig sektor påverkas resultatet av huruvida medborgare och företag har tillgång till, möjlighet att ge samtycke för och rätten att vägra, datadelning med offentlig sektor och tredje part. Men det finns ingen dimension som väger resultatet av olika länders initiativ för att utveckla digitaliseringen av offentlig sektor och skapa värde för medborgare och företag mot hur man hanterat faktiska och upplevda legala hinder utifrån GDPR och nationell lagstiftning eller praxis. 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

1.5 Internationella lösningar

De nordiska ländernas myndigheter har en lång tradition av att samla in data om individen, men det är inte helt enkelt 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-myndigheter och Danmark omstrukturering av sin offentliga administration har tidigt sökt att inkorporera EU:s uppmuntran till hållbar utveckling.[21]

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 tillåtelser 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 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.

[21] Joseph S and Avdic A "Where do the Nordic Nations' Strategies Take e-Government?" The Electronic Journal of e-Government Volume 14 Issue 1 2016 (pp 3-17), available online at www.ejeg.com

Det finns en viss konflikt mellan den lagstyrda modellens grundprinciper som fokuserar på rättssäkerhet och den marknadsanpassade förvaltningsmodellen med fokus på effektivitet, kundperspektiv och tillgänglighet. Utifrån marknadsperspektivet finns en pådrivande önskan om att onödiga eller föråldrade författningar som hindrar ett smartare arbetssätt ska förändras. Den juridiska utmaningen i en alltmer digitaliserad förvaltning är att tillvarata teknikens möjligheter och samtidigt behålla eller stärka rättssäkerheten.[22]

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

[22] Eriksson, J. Öppna myndigheten: Information och ärenden i e-förvaltningen, 2019, sid 11-18.

1.5.1 Finland

- Mycket hög ambitionsnivå både gällande att ge individen insyn och kontroll över sin personliga data och att ge staten möjlighet att nyttja denna data för att skapa en proaktiv offentlig sektor men insyn i individers möjliga framtida behov av offentliga tjänster.
- Att ge individer insyn via till exempel portaler som samlar information och tillhandahåller log-in möjligheter till egna sidor är en väl etablerad policy men det finns begränsningar i kontrollen individen får 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 och 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 problematiskt.

Finland ses som ett mycket ambitiöst land när det gäller att skapa förutsättningar för att nyttja data för sekundära användningar. Man arbetar aktivt för att i allt högre grad möjliggöra proaktivt agerande av 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.

Finlands vision om ökat nyttjande av stormängds- och öppna data utgår ifrån att juridisk reform är nödvändig och man hoppas att satsningar som görs kommer skapa incitament för detta och en samsyn på behoven och målen som kan delas av näringsliv, offentlig sektor, politiken och medborgaren.

Exempel på framgångar är att cirka 35 procent av befolkningen använder Mina Kanta-sidorna där medborgare kan se egna hälsouppgifter och recept och patienter kan 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 inte kontroll över om uppgifter får användas för forskning.

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 man se sina uppgifter som finns i vissa myndigheters register. Varje registerförare väljer vilka uppgifter som visas och anvisningar finns i anslutning till varje register för hur man kan rätta eller begära rättelse av felaktiga uppgifter.

Den finska visionen pekar mot att all information och data kan och bör göras tillgänglig via en enda plattform där åtkomst och anslutning av olika plattformar blir så sömlös och smidig som möjligt för användaren. I regeringens framtidsrapport från 2018 likställs digitaliseringen med möjligheten att skapa en offentlig sektor som agerar proaktiv till exempel med åtgärder för individers hälsoutveckling. För detta krävs dock tillgång till, och ett kombinerande av data från flera olika källor om individen. 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.

1.5.2 Frankrike

- Exemplen från Frankrike problematiserar en centraliserad statlig databas utifrån ett säkerhets- och integritetsperspektiv
- Ansvaret systemet lägger på individen att nyttja sin data från ett eget utrymme och på utvecklare att skapa en användarvänlig och engagerande miljö för insyn och kontroll av dataflödena verkar inte vara ett resultat av behov eller önskningar från vare sig medborgare eller företag.
- Utöver tekniska utmaningar så är utformningen av det egna datautrymmet av central vikt för att säkerställa att tjänster används och att data delas och används för att skapa än bättre tjänster.
- I Frankrike ligger en betydande del av fokus på att säkerställa att individer får en del av det värde som deras data skapar i form av bättre tjänster men även i form av ekonomisk kompensation eller medtjänande.

3.4.3.1 TES – Säkra elektroniska document

2016 beslutades skapandet av en massiv databas (titres électroniques sécurisés eller TES) av franska regeringen som innehåller 60 miljoner individers information. Det uttalade syftet var att bekämpa identitetsstöld men farhågor om att kombinera

data i databasen med data från andra källor har resulterat i återkommande debatter om databasens legalitet och integritetsskydd för personerna vars data inkluderas i databasen. Databasen innehåller samma information om individen som återfinns på ett ID-kort eller pass det vill säga, fullständiga namn, adress, ögonfärg, civilstånd, ett fotografi och fingeravtryck.

3.4.3.2 MesInfos

Konceptet MesInfos är Frankrikes motsvarighet till MinaData och den styrande grundidén är att om någon annan kan nyttja din data så borde du också kunna göra det, på det sätt du väljer. Från 2013 utfördes experiment i en testmiljö mellan privatpersoner och företag som lämnat ut kunddata till individerna som försetts med ett eget utrymme hos en leverantör av personliga molnlagringsutrymmen. Inledningsvis kunde man observera att tilliten till företagen förbättrades utifrån insynen individen fick om vilken data som företaget samlat in. 2016 utökades experimenten med fler deltagare för att utforska vilka nya tjänster, affärsmodeller och relationer kunde utvecklas. De stora utmaningarna var att identifiera lämpliga data, ställa in återställningsförfaranden via API:er och dokumentera teknikutvecklingsinsatser för att göra dem återanvändbara av tredje part.

Det personliga moln-utrymmet var även i fokus utifrån hur data skulle visualiseras och hur nya koncept skulle visas, göras begripliga och enkla att använda. Slutredovisningen av projektet visade hur viktigt själva gränssnittet är för kundretention (endast ca 10 % använde tjänsten efter 150 dagar)[23] men en annan fråga tog över i och med att GDPR infördes i Europa.

1.5.2.1 Regnbågsknappen och portabilitet

En separat studie som uteslutande fokuserade på efterlevnad av rätten till portabilitetslagstiftning inleddes i och med GDPR:s införande och som kallades för Rainbow Button-projektet. Franska MinaData-rörelsen förespråkade är att man bör gå ifrån knappar med olika färger för olika domäner (till exempel USA:s blå- och grönknappsinitiativ) då grundprincipen bör vara densamma det vill säga att organisationer i sitt kundgränssnitt, kan implementera ett standardiserat sätt för

[23] http://mesinfos.fing.org/wp-content/uploads/2018/12/MesInfos-2016-2018-final-research-report.pdf sid.18

människor att ladda ner sina personuppgifter i ett maskinläsbart och portabelt format.[24]

Arbetet har bland annat resulterat i en guidebok för dataportabilitet som pekar ut att enligt GDPR så måste data göras lättillgängliga i ett strukturerat, ofta använt maskinläsbart format så att individer kan välja att ladda ner sina data till en hårddisk eller överföra dem direkt till en tredje part.[25]Målet är nytta och ekonomiskt värde som kan härledas från individens personuppgifter bör delas mellan de som nyttjar data och de som producerat eller äger data.

1.5.3 Danmark

- Danmark utmärker sig i det avseende att man uppmuntrar till bred och öppen dialog mellan olika parter i frågan om ökad insyn för individen om personliga data.
- Betoningen i befintliga strategier är på insyn (offentlig transparens) snarare än på kontroll i nuläget och statliga hemsidor eller portaler är det verktyg som nämns mest.
- Danmark söker i regel andra vägar att uppnå önskvärda resultat än att utmana regelverk och lagar vilket underlättas av en stark datastrategi och av att man inte söker ge individen full kontroll över personliga data.
- När kontroverser såsom den kring danska databasen för allmänläkare uppstår så sker debatterna öppet och databasen stängdes ner efter påtryckningar från allmänheten.
- Lärdomen är att initiativ som förstärker kommersiella marknader för en viss typ av data utan att tillhandahålla datakällorna (medborgare) några kontrollverktyg kan leda till att intentioner och incitament ifrågasätts och olika intressen ställs mot varandra sent i en process.

1.5.3.1 Danmarks digitaliseringsstrategi

Danmarks digitaliseringsstrategi 2016 - 2020 uttrycker frågan om ökad insyn för medborgaren som en fråga om offentlig transparens. Medborgare och företag behöver ha enklare tillgång till data om dem själva som hålls av en specifik

[24] Comments on Data Portability guidelines | by Paul-Olivier Dehaye | MyData Journal | Medium
[25] http://mesinfos.fing.org/wp-content/uploads/2018/09/Notebook4_DataPortability_FV.pdf

myndighet. Denna tillgång borde innebära insyn i pågående ärenden, ansökningar, data och andra relationer med statliga institutioner. Strategin stannar dock vid insyn och översikt[26] och går inte in på eventuella modeller för att även öka kontroll över dataöverföring. Kontaktytan för att ta del av dessa tjänster anges som offentliga hemsidor eller portaler där användaren ska uppleva sig säker på hur sidorna ska navigeras snarare än som egna utrymmen som individen själv tillhandahåller.

Samarbetet med Kina via Beijing Genomics Institute (BGI) som etablerat sitt europeiska högkvarter i Köpenhamn, är ett exempel på hur Danmark söker nya möjligheter innanför ramen för de regelverk som reglerar områden såsom hantering av hälsodata. Danmark har identifierat hälsodata som ett viktigt utvecklingsområde men tillåter inte att danska vävnadsprover skickas utomlands. Samarbetet har istället fört utländska resurser och kompetenser till Danmark.[27]

1.5.3.2 Dansk Almen Medicinske Database

Den danska databasen för allmänläkare (Dansk Almen Medicinske Database (DAMD)) upphörde 2014 efter att integritets- och juridiska problem uppstod. Allmänläkarorganisationens kvalitetsenhet, Dansk Almenmedicinsk Kvalitetsenhed (DAK-E) fick framträdande roll i datainfrastrukturen med ansvar för den dagliga driften av DAMD och bland annat, leverans av kvalitetsrapporter till allmänläkarna.[28] En konflikt uppstod så småningom då vissa allmänläkare uttryckte oro för huruvida data skulle användas för mer än den ursprungliga tanken med insamlingen och eventuellt i vissa kommersiella syften. Konflikten resulterade i att DAMD stängdes ner 2014 efter att farhågor uppmärksammats i offentlig debatt och spridit sig till parlamentariska diskussioner kring lagligheten av datainsamlingen i sig.

Medborgarna krävde att deras uppgifter skulle raderas och hösten 2014 beslutades det att datautvinningen troligen var olaglig och datainsamling avbröts. 2017 nådde allmänläkarna och regionerna en ny överenskommelse som öppnade för inhämtning av utvalda typer av data och för utvalda ändamål. Exemplet syftar till att visa att sömlös datainhämtning från apotek, laboratorier och kliniker, som

---

[26] https://en.digst.dk/media/14143/ds_singlepage_uk_web.pdf sid. 22

[27] BGI opens genome research center in Europe | EurekAlert! Science News

[2828] Dangers of the digital fit: Rethinking seamlessness and social sustainability in data-intensive healthcare, DOI: 10.1177/2053951717752964, Sarah Wadmann, Klaus Hoeyer 2018 sid. 8

förstärker kommersiella marknader för hälsodata utan att tillhandahålla datakällorna (patienterna) några kontrollverktyg, kan leda till att intentioner och incitament kan ifrågasätts och att konflikter mellan olika intressen uppstår.

1.5.4 Norge

- Norge liknar i viss mån Finland i hur väl man etablerat portaler som skapar en upplevelse av sömlös hänvisning och tillgång till offentliga tjänster.
- Norge utforskar förutsättningar för ökad insyn och kontroll för individen gällande personliga data och uppdraget *Digital Assistent* som slutredovisas i september 2021 har liknelser med det svenska uppdraget på området.
- Norge, i likhet med andra länder genomför medborgarundersökningar som visar att det råder oklarhet bland medborgare om vad ett ökat ansvar för sina personliga data kan komma att innebära och hur de ska användas.

Enligt OECD:s Digital Government Review av Norge så bör utvecklingen av en datadriven offentlig sektor i Norge fokusera på det grundläggande behovet av att bygga och upprätthålla medborgarnas förtroende. Ett bra sätt att göra detta på enligt OECD är att etablera mekanismer som tillåter medborgare ökad tillgång till sina personliga data som hålls inom offentlig förvaltning och som möjliggör för insikt i vem som kommer åt ens data och i vilket syfte.[29]

1.5.4.1 Norge.no

Norge använder sig av en gemensam portal för alla medborgartjänster, Norge.no som länkar till digitala offentliga tjänster inom alla sektorer och nivåer av offentlig förvaltning i Norge i likhet med Finlands soumi.fi. Dessa digitala tjänster kan filtreras via en sökfunktion, en ämnesmeny eller åtta livshändelser.[30] Digital kommunikation mellan myndigheter och kommuner och medborgare ses som en central tjänst och Norges digitala brevlådesystem ges mycket utrymme på portalen.

[29] https://www.oecd.org/gov/digital-government/digital-government-review-norway-recommendations.pdf sid. 23-25
[30] https://www.norge.no/en/

1.5.4.2 Altinn

Norska Skatteverket, Norska Statistikbyrån och Brønnøysund Register Center startade 2002 en portal kallad Altinn[31] för att underlätta finansiell rapportering. Idag är Altinn en väletablerad och omfattande plattform både i antal anslutna myndigheter och kommuner men även i antal digitala tjänster. Tjänsterna är både rent informativa i karaktär men också av transaktionskaraktär, det vill säga att medborgare och företag kan både ta emot och skicka information genom tjänsterna. En framgångsfaktor som gärna lyfts fram är att portalen tidigt drevs utifrån kundperspektivet och inte fokuserade på tekniska detaljer samt att portalen möjliggör back-office samverkan mellan olika myndigheter på ett strukturerat och säkert sätt.

1.5.4.3 Digital Assistent

I Norges Digitala Agenda återges ambitionen att medborgare ska, i den mån det är möjligt, ha kontroll över sina egna data. Personliga data registreras och hålls i allt större volymer vilket å ena sidan möjliggör för att kombinera med annan data för att skapa medborgarvärde men å andra sidan ökar även behovet av att skydda data. Mot denna bakgrund har Norska Direktoratet för digitalisering fått i uppdrag att utvärdera koncept för förverkligande av en medborgarorienterad lösning av en virtuell assistent, i linje med åtgärderna i digitaliseringsstrategin. Konceptutformningen ska redovisas 1 september 2021.

Begreppet digital assistent har inte tydligt definierats eftersom man ännu inte vet vad behovsbilden är. Man utreder om det är en portal för sammanlänkande tjänster som behövs, om det är tillgång till personliga data som hålls av offentlig förvaltning som efterfrågas av medborgarna, om det är mer individualiserade offentliga tjänster man vill ha eller om företagsbehov av mer sammanlänkade tjänster borde prioriteras.

I tidiga resultat från medborgarundersökningar upplever man att medborgare gärna ser att man själv kan bestämma vad som ska och inte ska delas och att man vill ha offentliga tjänster som är skräddarsydda efter individens behov och situation. Samtidigt visar de preliminära svaren på att det inte görs så mycket

[31] https://www.altinndigital.no/

reflektion bland medborgarna om konsekvenserna av datadelning och vad det innebär att ha tillgång till sina egna uppgifter.[32]

1.5.5 Storbritannien

- I Storbritannien utgör möjliga samhällsekonomiska vinster med ett system för ökad insyn och kontroll en betydande del av motivationen bakom varför frågan utreds.
- Offentlig sektor bör säkra en digital infrastruktur för delning av personuppgifter som skapar tillit till modellen
- Det krävs en ökad medborgerlig förståelse för vad personliga data är och vilka konsekvenser individuell kontroll över personliga data kan få
- Det saknas exempel på realiserad nytta för individer och ekonomiska incitament för företag att medverka till att skapa en ny infrastruktur för hur data nyttjas och tjänster erbjuds.
- Det krävs en koordinerande enhet för personuppgiftsmobilitet med representanter från regeringen och som arbetar efter en framtagen agenda för infrastruktur och standarder, kompetens och adaptiva regelverk.
- En kompletterande agenda bör tas fram i samverkan med näringslivet som fokuserar på utveckling av tjänster och applikationer.
- I avsaknad av ekonomiska motiv bör företag uppmuntras att delta utifrån att det handlar om utforskande innovationsarbete som hamnar under företagens arbete med samhällsansvar.

Engelska ministeriet för digitalisering, kultur, media och sport (DCMS) undersökte potentialen för att stimulera innovation och konkurrens genom personuppgiftsportabilitet 2018. Den resulterande rapporten[33] menar på att GDPR inte beskriver hur värde bör genereras från dataportabilitet vilket gör det oklart hur den enorma potentialen med personuppgifter ska förverkligas.

Rapporten lyfter fram fem kärnfrågor med rekommendationer kopplade till dessa. Offentlig sektor bör säkra en digital infrastruktur för delning av personuppgifter som skapar tillit till modellen för delning (kärnfråga 1). Det krävs även en ökad

[32] Från erfarenhetsutbytesmöte mellan arbetsgruppen och DigDir Norge 20201120
[33] DCMS_Ctrl-Shift_Data_mobility_report_full.pdf (ctrl-shift.co.uk)

medborgerlig förståelse för vad personliga data är och vilka konsekvenser dess hantering kan ha, positiva såväl som negativa (kärnfråga 2). Vidare behöver staten och lagstiftare kompetensutveckling inom området dataportabilitet och öka förståelsen för sambandet till andra delar av den ekonomiska och samhälleliga utvecklingen för att där utefter kunna anpassa regelverk och stödja den önskade utvecklingen (kärnfråga 3). Det behövs fler tjänster och applikationer som gör det möjligt för individer att använda personliga data för att skapa värde för sig själva och andra (kärnfråga 4) och företag saknar bevis för värdet i innovationsmöjligheterna på området och ombeds i praktiken att ta en risk och bära kostnaden kopplad till att stöpa om affärsmodeller i en redan osäker affärsmiljö (kärnfråga 5). Rekommendationer för att realisera värdepotentialen utgår ifrån dessa kärnfrågor och kan delas in i 3 huvudrekommendationer;

1. Inrättande av en koordinerande enhet för personuppgiftsmobilitet – enheten ska effektivt kunna driva samverkan mellan olika intressentgrupper och bör inkludera regeringsrepresentanter eller förses med strategiskt stöd.
2. En utvecklingsagenda för personuppgiftsmobilitet – Den koordinerande enheten ska fokusera på infrastruktur och standarder, kompetens och adaptiva regelverk.
3. Affärsledd personuppgiftsmobilitet agenda – en kompletterande agenda bör tas fram i samverkan med näringslivet som fokuserar på utveckling av tjänster och applikationer.

1.5.5.1 Midata

Redan 2011 initierade Storbritanniens departement för *Business, Innovation and Skills* det så kallade midata programmet som utforskade olika aspekter av dataportabilitet för personliga data.[34] Syftet var att ge konsumenter tillgång till data som tjänsteleverantörer samlade in om dem och viss möjlighet för dem att använda denna data i andra syften. Intentionen var att skapa en plattform för innovation samtidigt som individen stärktes med förmågan att agera på nya sätt inom den digitala data-drivna ekonomin.

Likt det franska experimentet MesInfos så baserade midata på att företag frivilligt gjorde data tillgängligt för den enskilde kunden. Ett midata innovationslabb

[34] https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment

skapades inom vilket dessa företag kunde utforska och utveckla innovationsmöjligheter inom ekosystemet i samarbete med ett multidisciplinärt team. Ett resultat var ett QR-kodssystem där kunder av elföretag kunde skanna koden på sin räkning och få detaljerad information om sin förbrukning. Tanken var att detta skulle driva på konkurrensen mellan företag som skulle kunna skräddarsy erbjudanden utifrån individuella förbrukningsmönster och man ansåg inte att omställning för att kunna erbjuda QR-koder bar någon väsentlig kostnad för företagen.[35] Ett problem var personers relativt låga intresse i sina elförbrukningsmönster och i QR-koder generellt vilket är ett återkommande tema inom frågan om ökad insyn och kontroll det vill säga vad är det man förväntar sig att individer ska göra med sin ökade insyn och nivå av kontroll över sin data. I de flesta fall verkar man vara nöjd med att det går att göra något utan att man för den sakens skull gör det.

Insikterna från programmet var att framsteg uppnås snabbare om målet och syftet för deltagande aktörer att engagera sig i personliga datas mobilitet är att det är en del av företagens samhällsansvar och att det erbjuder en möjlighet att arbeta med innovation.[36] Detta eftersom det i de flesta fall saknas ett tydligt ekonomiskt affärsvärde eller ny affärsmöjlighet för företag att göra deras kunddata tillgängligt. Det visades också vara lättare att skapa deltagarengagemang från företag om det fanns högt uppsatt politisk representation närvarande i olika intressent- och planeringsmöten.

1.5.6 USA

- Blåknappsinitiativet är ett exempel på hur insyn- och kontrollinitiativ kan vara mycket framgångsrika om företagen ser området som en värdig sakfråga (veteraners hälsa) och om politisk styrning och stöd är tydligt.
- Grönknappsinitiativet är ett exempel på där skapandet av tekniska standarder och samverkan inom en bransch kan leda till bättre tjänster och hur delning till tredje part kan skapa innovativa nya tjänster.

[35] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/276198/bis-14-519-midata-programme-feasibility-study-on-use-of-qr-codes-in-energy-sector.pdf sid. 18

[36] https://www.gov.uk/government/publications/qr-code-use-in-energy-sector-midata-programme-study

1.5.6.1 Blåknappsinitiativet

2010 lanserades den blå knappen av U.S. Department of Veteran Affairs och Obamaregimen i syfte att ge veteraner möjligheten att ladda ner sina hälsojournaler från webbportalen *MyHelathVet*[37]. 2013 expanderades tjänsten till att inkludera ett standardiserat, maskinläsbart dataformat. Genom att logga in kan patienten få tillgång till olika typer av personliga vårddata som uttag av medicin, genomförda vaccinationer för sig själv men också för sina barn, tillgång till hela sin historiska vårdjournal med mera. Patienterna kan även dela sin personliga data med andra som de har förtroende för; familjemedlemmar, släktingar eller sin doktor eller vårdinrättning.

USA har infört ekonomiska incitament för att få vårdinrättningar och vårdgivare att använda sig av elektroniska journaler i syfte att underlätta för patienterna och ge dem tillgång till elektroniska hälsodata. U.S. Department of Health and Human Services ansvarar för att ha tagit fram ramverk och riktlinjer för användandet, de tekniska installationerna samt kommunikation gentemot användarna. År 2019 använde ca 95% av USA:s vårdinrättningar elektroniska hälsodata[38] och cirka 81 % av de som loggat in och använt sig av tjänsterna fann dem värdefulla.[39]

Blåknappsinitiativet är ett exempel på ett initiativ med stark politisk backning och en allokerad budget från politiskt håll samtidigt som temat eller målgruppen som stod att tjäna mest av initiativet enkelt kunde ses som ett värdigt område att engagera sig i för privata aktörer även om det inte fanns ett tydligt affärsintresse för att ingå i initiativet.

1.5.6.2 Grönknappsinitiativet

Två år efter blåknappsinitiativet lanserades det så kallade grönknappsinitiativet 2012. Detta initiativ gav individer tillgång till detaljerade elförbrukningsbeskrivningar vilket i princip utgjorde energirevisioner som identifierade ineffektivitet och möjligheter till besparingar för privata såväl som för kommersiella kunder hos elbolagen.[40] Elbolagen möjliggör nerladdning av specifikationerna genom en grön knapp på deras hemsidor (därav namnet).

---

[37] https://www.myhealth.va.gov/mhv-portal-web/web/myhealthevet/about-mhv
[38] https://www.healthit.gov/sites/default/files/page/2019-04/AHAEHRUseDataBrief.pdf
[39] https://www.healthit.gov/infographic/value-consumer-access-use-online-health-records
[40] https://www.energy.gov/data/green-button

Informationen kan delas direkt med tredje part som utvecklar tjänster där du kan jämföra din förbrukning med lokala förbrukningsmönster som skapas av kommuners öppna data.

Grönknappsinitiativet är ett exempel på där tekniska standarder och samverkan inom en bransch kan leda till bättre tjänster och skapa värde även om inget av elföretagen såg detta som en möjlig konkurrensfördel eller hade specifika visioner för hur systemet skulle kunna skapa dem nya affärsmöjligheter. Initiativet baserades på en gemensam teknisk standard, ESPI (Energy Services Provider Interface) som beskrev hur man representerar data om energianvändning i ett XML-format och hur man möjliggör utbyte av den informationen mellan elbolagen och tredje part för konsumenternas räkning. Tillsammans definierade dessa ett flexibelt filformat för initiativet baserat på ratificerade standarder från North American Energy Standards Board. Inom tre år hade över 60 miljoner hushåll, tillgång till den gröna knappen via sina elbolag.

1.5.7 Indien

- Uppfattningen är att Individuell kontroll av personliga data anses vara ett sätt att öka antalet aktörer som genererar värde på marknaden och ökar den ekonomiska inkluderingen av Indiens befolkningsmängd.
- Individer kapacitet att avgöra vad som utgör rätt användning av sina personuppgifter kallas för *individuell bemyndigande genom data*
- Tre viktiga byggstenar behövs för att skapa ökad inkludering genom ökad insyn och kontroll för individen: möjliggörande regelverk, standarder inom avancerade teknologier och nya typer av offentliga och privata organisationer med incitament att agera i medborgarens bästa intresse.
- En privat samtyckeshanterare föreslås säkerställa att individer kan ge samtycke enligt en innovativ digital standard för varje enskild datapunkt som delas och arbeta för att skydda individens datarättigheter.
- Delning baserad på samtycke, som går att granska och återkalla, utgör ett första steg inte en slutdestination
- Samtyckehanterare ska kunna ansluta till ett nätverk av informationsleverantörer och användare och konkurrera om olika kundsegment genom design och användarvänlighet av den yta individen använder för insyn och kontroll av sina data, det egna utrymmet.

Indiens Data Empowerment and Protection Architecture (DEPA)[41] är ett säkert, samtyckebaserat ramverk för datadelning som syftar till att påskynda ökad ekonomisk inkludering. Ramverket baseras på uppfattningen att individer ska ha kontroll över hur deras personuppgifter används och delas. Det är utformat med tron att kontroll över data kan ge indiska medborgare möjlighet att förbättra sina egna liv. Personliga data anses kunna hjälpa människor att informera och bygga förtroende hos viktiga institutioner som tillhandahåller livsförändrande tjänster, till exempel sjukhus, banker eller framtida möjliga arbetsgivare. Det anses då orimligt att inte också ge individer ökad kontroll över deras uppgifter då de själva anses kunna bedöma rätt användning av sina personuppgifter. Individer bör då ha enkel tillgång till data om en själv och möjlighet att enkelt dela denna data vidare. Tre viktiga byggstenar behövs enligt DEPA: möjliggörande regelverk, standarder inom avancerade teknologier och nya typer av offentliga och privata organisationer med incitament att agera i medborgarens bästa intresse.

DEPA ämnar ge människor möjlighet att sömlöst och säkert komma åt deras data och dela med tredje part. En ny typ av institution, en privat samtyckeshanterare ska säkerställa att individer kan ge samtycke enligt en innovativ digital standard för varje enskild datapunkt som delas säkert med nyskapade standard-API:er. Dessa samtyckehanterare arbetar också för att skydda individens datarättigheter.

En viktig aspekt av DEPA är att den kombinerar offentlig digital infrastruktur med privat marknadsstyrd innovation. Det skapar ett konkurrenskraftigt ekosystem där alla nya samtyckehanterare kan ansluta till ett nätverk av informationsleverantörer och användare där datadelning sker via samtycke som går att granska och återkalla. Samtyckehanterare kan konkurrera om olika kundsegment genom design och olika leveransmetoder för att få informerat samtycke och experimentera med olika affärsmodeller. Samtycke kan inte utgöra grunden för all delning av data men det är ett kraftfullt första steg för att stärka individen genom ökad kontroll av hens data.

[41] Data Empowerment and Protection Architecture - Draft for discussion, seeking comments | NITI Aayog