Målbillede for digitalt samtykke og frabedelse

(målbillede version 1.0)

Change log

Dato	Initialer	Primære ændringer
01.02.22	KLHEJ	Godkendt uden bemærkninger af den fællesoffentlige styregruppe for digital kommunikation

Indhold

0. Introduktion

Formål

Dette dokument beskriver et fællesoffentligt målbillede for tværgående digitalisering af samtykke og frabedelse.

Formålet med digitalisering af samtykker og frabedelser er primært at give borgere og medarbejdere overblik over relevante samtykker og frabedelser samt mulighed for at administrere disse til at sikre overholdelse af relevant lovgivning på området. Dette kan opnås ved at udvikle en central service, der kan understøtte digital håndtering af samtykker og frabedelser i den offentlige sektor samt understøtte transparens i deres anvendelse.

Målbilledet dækker hele samtykkets livscyklus: Fra medarbejderens indhentning og borgerens afgivelse, over deling og genbrug på tværs af relevante organisationer og borgerens mulighed for at få et tværgående overblik og indblik i, hvilke organisationer der anvender hvilke samtykker, til borgerens mulighed for at trække et samtykke eller en spærring tilbage eller den ansvarlige organisations håndtering af samtykkets udløb, arkivering og sletning.

Samtykke giver retsgrundlag for databehandling og datadeling. Samtykke anvendes desuden som retsgrundlag for sagsbehandling jf. fx Servicelovens krav til samtykke som retsgaranti og som retsgrundlag for behandling af personer, fx behandling af patienter, jf. Sundhedsloven. **Frabedelse** giver retsgrundlag for begrænsning af datadeling gennem spærring og privatmarkering af data inden for eksempelvis sundhedsdomænet, hvor det er en rettighed funderet i Sundhedsloven. Målbilledet dækker således over en række områder med stor indbyrdes forskel i formålet med anvendelsen af samtykker og frabedelser. Fælles for dem alle er imidlertid, at der er tale om tilladelser til at foretage en handling, som ikke er hjemlet i lovgivningen, henholdsvis blokere for visse former for behandling af persondata, som er hjemlet i lovgivningen.

Fælles arkitektur, standarder og infrastruktur skal gøre det muligt via en (logisk) central service at dele samtykker og frabedelser på tværs af sektorer og domæner, således at der kan leveres et samlet overblik til borgere, og medarbejdere kan få overblik over relevante samtykker. Desuden skal det bidrage til at forbedre datadeling og adgangsstyring. Implementering skal ske gradvist med fokus på, hvor det skaber værdi, og hvor der er modenhed.

Som første skridt etableres en infrastrukturløsning i form af et minimum viable product (MVP), der implementeres på udvalgte pilotområder. Scope omfatter i første omgang primært den offentlige sektor med fokus på anvendelse i relation til fællesoffentlige samarbejder og udvalgte private aktører, som er direkte knyttet til offentlig opgaveløsning (fx privatpraktiserende læger og forsyningsselskaber) og konkrete projekter. På sigt kan scope eventuelt udvides til den private sektor i bredere forstand afhængig af nærmere analyse og aftale mellem de relevante parter.

Der er som udgangspunkt lagt op til, at der skal være frihed til, at man i de enkelte domæner selv kan bestemme ambitionsniveauet for, hvor avancerede implementeringer man foretager, så man fx både kan genbruge eksisterende samtykkeløsninger baseret på ustrukturerede dokumenter (fx pdf-format), der har begrænset potentiale i forhold til automatisering, eller udvikle mere avancerede løsninger baseret på strukturerede dokumenter (fx xml-format), som kan understøtte øget automatisering.

Målbilledets fokus er på fremadrettet digitalisering, således at eksisterende samtykker og frabedelser som udgangspunkt ikke migreres til den kommende nationale løsning. Hvis et domæne ønsker at dele eksisterende samtykker via denne infrastruktur og udstille disse til et borgervendt overblik, skal dette dog også være muligt.

Mundtlige og stiltiende samtykker digitaliseres kun i det omfang, det giver forretningsværdi. Dette vurderes for konkrete samtykker i de enkelte domæner.

Målbilledet omfatter support til både borgere og medarbejdere samt alternative muligheder for ikke-digitale borgere.

Målbilledet følges op med fastlæggelse af fælles referencearkitektur, begrebsmodel, informations- og datamodel, udvekslingsformat, snitfladespecifikationer, sikkerhedsmodel og forretningsmæssige og tekniske krav til SLA (service-level agreement) for de infrastrukturløsninger, fagsystemer og borgervendte løsninger, der indgår i det samlede digitale økosystem. Blandt andet skal der udarbejdes en fælles model for, hvordan man beskriver et samtykkes genstands- og virkefelt, herunder hvor det er gældende, og hvor det ikke er, for hvem det gælder, og i hvilken periode det gælder.

Målgruppe

Målbilledet henvender sig til beslutningstagere. Projektledere og teknisk orienterede læsere, som fx it-arkitekter, anbefales ligeledes at læse målbilledet for at få et overordnet billede af ambitionerne for fællesoffentlig funktionalitet til håndtering af samtykker og frabedelser.

Baggrund

Udarbejdelsen af dette målbillede udspringer af den fællesoffentlige digitaliseringspagt fra 2019, hvor det blev aftalt at igangsætte et analysearbejde om digitalt samtykke. Udfordringer med samtykke har været oppe i mange sammenhænge, og initiativer til løsning af disse udfordringer indgår nu i *Fællesoffentligt 2021-initiativ om bedre digital understøttelse af samtykke* og i *Aftaler om kommunernes og regionernes økonomi for 2022*, hvor der er afsat midler til et videre arbejde med fælles arkitektur og specifikationer samt udvikling af fælles infrastrukturkomponenter i form af en central MVP-løsning. Der er nær sammenhæng mellem samtykke og frabedelse, hvorfor sidstnævnte også er genstand for nærværende målbillede.

Samtykkeprojektet og målbilledet er forankret i den fællesoffentlige styregruppe for digital kommunikation og en projektgruppe med deltagelse af Digitaliseringsstyrelsen, KL og Danske Regioner. Målbilledet er udarbejdet i et nært samarbejde med en arbejdsgruppe, som foruden repræsentanter fra ovenstående organisationer tæller repræsentanter fra Sundhedsdatastyrelsen, Region Hovedstaden, Region Midtjylland, Region Syddanmark, ATP, KOMBIT, Københavns og Odense Kommune, Styrelsen for Dataforsyning og Effektivisering samt Udviklings- og Forenklingsstyrelsen.

Parallelt med arbejdet med dette målbillede har sundhedsområdet udarbejdet et målbillede for samtykke og frabedelse i forbindelse med databehandling inden for sundhedsdomænet. Der har været en tæt dialog og koordinering mellem de to projekter. Indsigter fra sundhedsområdet er således også indeholdt i nærværende målbillede for digitalt samtykke og frabedelse, hvis genstandsfelt også omfatter databehandling på sundhedsområdet.

Der eksisterer en række forretningsmæssige og tekniske lighedspunkter mellem samtykke, frabedelse og fuldmagt, hvorfor der vil ske en tæt koordinering mellem nærværende projekt

og arbejdet med den kommende fællesoffentlig fuldmagtsløsning, som er igangsat senere og derfor befinder sig på et tidligere stadie i analysefasen. Fuldmagtsarbejdet vil ved relevante milepæle og opstart af konkrete leverancer såsom begrebs- og datamodeller, referencearkitektur samt egentlig udvikling, vurdere i hvilket omfang byggeblokke fra samtykke og frabedelse kan genbruges, eventuelt udvides så de også kan dække fuldmagtsbehov. Det forventes, at fuldmagtsområdet kan genbruge væsentlige dele af målarkitektur, specifikationer og løsningskomponenter og dermed sikre optimal synergi og de bedst mulige løsninger set fra et brugerperspektiv.

I forlængelse af dette målbillede udarbejdes en referencearkitektur, som går i dybden med forretnings- og teknisk arkitekturen for digitalt samtykke og frabedelse. Herunder overordnede forretningsmønstre med roller, flows og forretningsregler og generelle tekniske implementeringsmønstre med applikationskomponenter, services og snitflader. Rammerne for brugerstyring uddybes i en sikkerhedsmodel. Et udkast til referencearkitekturen skal anvendes som grundlag for udviklingen af den centrale MVP-løsning og decentral implementering i pilotprojekter. Når udviklingen af MVP er gennemført, og de første pilotafprøvninger er gennemført, skal målbilledet, referencearkitekturen og diverse arkitekturprodukter opdateres eller færdiggøres på baggrund af de høstede erfaringer med MVP og piloter. Det er forventningen, at der samtidig kan ske en indarbejdelse af fuldmagtsområdet, således at fx referencearkitekturen kan dække alle tre typer af viljestilkendegivelser i form af samtykke, frabedelse og fuldmagt.

Centrale begreber

Dette målbillede handler om, hvordan der kan gives eller fjernes hjemmelsgrundlag for en anden fysisk eller juridisk persons handlinger.

Begrebet **viljestilkendegivelse** anvendes som et fælles overbegreb for samtykke, frabedelse og fuldmagt. En viljestilkendegivelse er i det fællesoffentlige begrebsarbejde beskrevet som en "tilkendegivelse, der udtrykker den berørte parts vilje til at skabe, udløse, bevare eller fjerne en rettighed, bemyndigelse, eller en pligt". I denne sammenhæng indebærer en viljestilkendegivelse, at en person med sin viljestilkendegivelse bemyndiger en myndighed eller en person til at foretage en konkret behandling, iværksættelse af en foranstaltning eller forløb, behandling af data eller indskrænkning af behandleres i sundhedsvæsenets adgang til viljestilkendegiverens data.

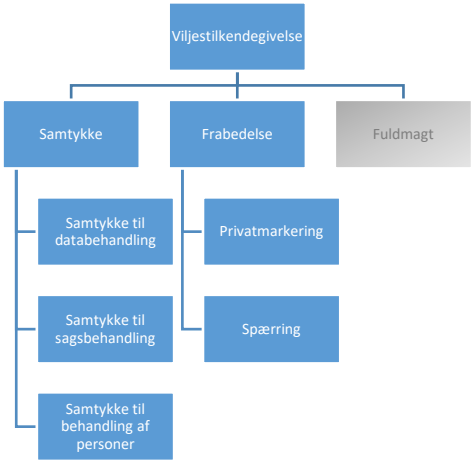
Et **samtykke** er brugerens frivillige tilladelse til, at en eller flere aktører må foretage en given handling, eksempelvis at lade en myndighed udlevere data om brugeren til en anden myndighed.

Inden for sundhedsdomænet har enheder og medarbejdere med en behandlingsrelation til borgeren hjemmel i lovgivningen til at tilgå og behandle en borgers persondata, medmindre borgeren har foretaget sig en **frabedelse** i form af en privatmarkering eller en spærring. Ved en **privatmarkering** har borgeren tilkendegivet, at alle eller udvalgte oplysninger skal underkastes en særlig beskyttelse**.** Et eksempel er oplysninger registreret i forbindelse med en igangværende behandling for stofmisbrug, som borgeren ikke ønsker skal være umiddelbart synlige for andre sundhedsfaglige end dem, der er involveret i misbrugsbehandlingen. Frabedelse kan også forekomme i form af en **spærring**, der har til hensigt at sikre, at en bestemt person, som arbejder i sundhedsvæsenet, ikke kan indhente oplysninger om den borger, som oplysningerne drejer sig om. Brug af frabedelse inden for andre domæner indgår ikke nærværende målbillede, men scope for målbilledet kan udvides, hvis afdækning og afklaring mellem de relevante domæner og de fællesoffentlige parter

leder frem til, at dette er formålstjeneligt. Både samtykke og frabedelser afgives fra en borger til en eller flere fagpersoner eller myndigheder.

Fuldmagt er også en type viljestilkendegivelse, men denne vil, som nævnt ovenfor, først blive nærmere behandlet på et senere tidspunkt.

Nedenstående figur (figur 0.1)giver et overblik over sammenhængen.



Figur 0.1 - Centrale begreber for samtykker og frabedelser

Som led i projektet udarbejdes der en samlet begrebsmodel for samtykke og frabedelse samt relevante relaterede begreber. Oven på begrebsmodellen bliver der desuden udarbejdet en informations- og en datamodel samt et standardiseret udvekslingsformat

1. Styring

Interessenter

De primære aktører og bestillere af dette målbillede er de fællesoffentlige parter – stat, kommuner og regioner – men derudover er der en række interessenter, der har en afgørende betydning for dette målbillede og en stor interesse i den ønskede transformation. Det gælder både i forhold til behovet for det og i forhold til rammerne for dets realisering.

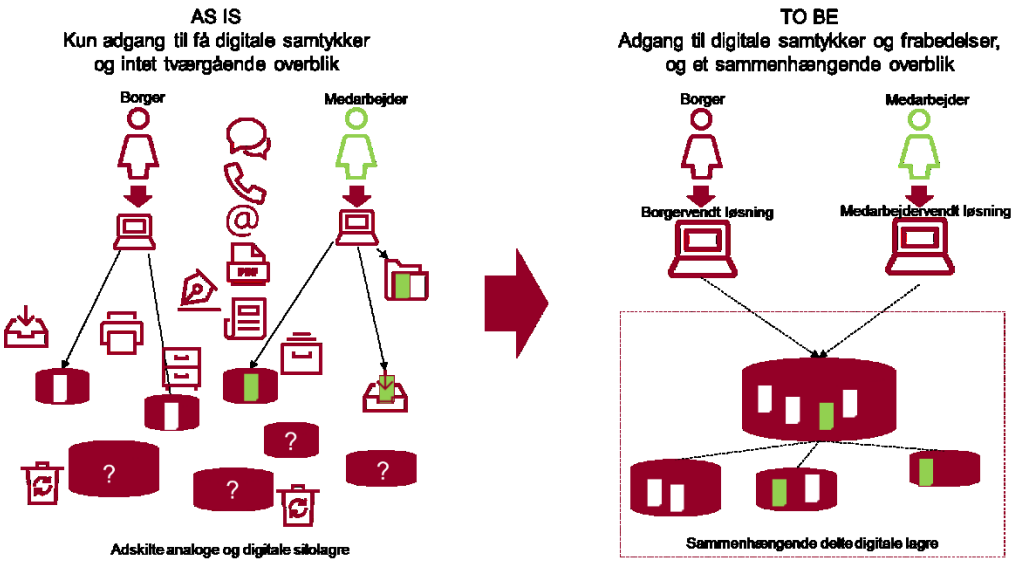
Målbilledet defineres i forhold til en meget stor og kompleks mængde interessenter i forhold til samtykke. De mest centrale er:

- **Borgere eller pårørende**, der agerer på vegne af en borger, som skal kunne afgive et samtykke, ønske en frabedelse eller skal kunne trække samme tilbage. Omfatter ikke-digitale borgere, som fx skal kunne afgive samtykke mundtligt eller skriftligt til en medarbejder eller via en partrepræsentant ved hjælp af fuldmagt.
- **Organisationer,** der agerer som dataansvarlige og/eller –behandlere som fx myndigheder, institutioner og private virksomheder, som har behov for at kunne indhente og håndtere anvendelsen af samtykker og frabedelse i forbindelse med deres opgaveløsning. Organisationerne er ansvarlige for at kunne sikre interoperabilitet og dokumentere lovmedholdelighed inden for egne organisationer og domæner samt på tværs af den offentlige og private sektor.

- **Rammesættende myndigheder,** som stiller krav til anvendelse af samtykke, herunder rammelovgivning som fx databeskyttelsesforordningen og persondataloven såvel som domænelovgivning som fx sundhedsloven eller lov om social service. Disse er ansvarlige for at kunne sikre juridisk (og semantisk) sammenhæng.
- **Skabelon-ansvarlige,** der udvikler og vedligeholder skabeloner til samtykker, frabedelser og fuldmagter til anvendelse i et eller flere veldefinerede domæner, fx inden for det kommunale område eller sundhedsområdet.
- **It-leverandører**, der leverer it-systemer til det offentlige, er ansvarlige for at følge målbillede og den ønskede transformation. It-leverandørerne har en interesse i, at målbilledet fastlægger nogle klare overordnede rammer og retningslinjer for det efterfølgende mere detaljerede arkitektur- og implementeringsarbejde, og at håndteringen af samtykker og frabedelser i eksempelvis lokale fagsystemer kan spille sømløst sammen med de fællesoffentlige løsninger for samtykker og frabedelser
- **Standardiseringsorganisationer,** der arbejder for udvikling og anvendelse af tekniske specifikationer, som kan sikre åben konkurrence og teknisk (og semantisk) interoperabilitet.

Forretningsmål – hvad driver udviklingen?

Udgangspunkter er den aktuelle situation, hvor en borger har vanskeligt ved at fremfinde et samtykke, få et tværgående overblik eller trække et samtykke tilbage, og hvor en medarbejder tilsvarende kan have svært ved at få et overblik og dele det med relevante parter. Nedenstående figur (figur 1.1) illustrerer den ønskede forandring.



Figur 1.1 - Den ønskede forandring fra papir og silostruktur til digitalisering og sammenhæng på tværs

De væsentligste drivere for målbilledet er bredt forankrede ønsker om:

- At gøre det nemmere for borgere at afgive, tilbagekalde og få overblik over samtykker og frabedelser samt for medarbejdere og organisationer at indhente, anvende og administrere samtykker og håndtere frabedelser.
- At understøtte tværgående processer og datadeling gennem samtykke som retsgrundlag, der hvor det ikke er muligt eller relevant at basere sig på lovhjemmel.
- At understøtte tværgående processer og datadeling med henblik på at gøre det lettere for myndighederne at efterleve lovgivningen, herunder forvaltningsloven, sundhedsloven og ikke mindst databeskyttelsesforordningen.
- At udnytte potentialerne i personrelaterede data bedre offentligt og privat.

Brugerbehov og forretningsbehov

De centrale forretningsbehov i forhold til en sammenhængende håndtering af samtykke og frabedelse, som nøgleinteressenterne har formuleret i fællesskab, er:

- Samtykker og frabedelser skal kunne håndteres i processer, hvor de enkelte procestrin håndteres af forskellige parter, hvilket forudsætter løs kobling mellem dannelse og anvendelse af samtykker og frabedelser, således at et samtykke fx ikke er bundet til ét specifikt fagsystem.
- Samtykker og frabedelser skal kunne deles, være tidstro og kunne fortolkes, så parterne altid kan anvende det autoritative samtykke og frabedelse, hvilket forudsætter fælles datamodel.
- Samtykker og frabedelser skal afspejle det enkelte domæne eller sagsområde, hvilket forudsætter fleksibilitet for at kunne håndtere forskellige processer, regler og juridiske krav, som skal understøttes, fx også afgivelse på vegne af andre såsom mindreårige. Behovet for fleksibilitet vedrører dermed også de skabeloner, som ligger til grund.
- Skabeloner skal være underlagt klar governance med versionsstyring, så man kan sikre, at samtykker, der baseres på en skabelon, er lovmedholdelig, overholder fælles standarder og har den rette kvalitet, samt sikre at der ikke opstår for mange varianter og ikke mindst, at de er bredt anerkendte blandt de aktører, der skal anvende dem.
- Samtykker og frabedelser skal kunne håndteres let, korrekt og sikkert af både mennesker og maskiner, hvilket forudsætter, at de relevante dele er struktureret til at understøtte dette.
- Samtykker og frabedelser skal kunne arbejde sømløst sammen med den fællesoffentlige infrastruktur, som f.eks. Digital Post, MitID, NemLog-in, Mit Overblik og Digital Fuldmagt.

Værdiskabelse

Realisering af målbilledet vil skabe værdi på flere måder. Det vil bidrage til, at borgerne, virksomhederne og medarbejderne møder offentligt digitale løsninger af høj kvalitet, som sikrer tryghed, transparens, overblik og effektivitet. Der er således en forventning om en række kvalitative, ikke-økonomiske gevinster. Dette gælder både i forhold til borgernes rettigheder og tillid, qua understøttelse af indsatsen for at sikre større transparens i anvendelsen af borgernes data. Tilsvarende understøttes mulighederne for automatisk

udveksling af data, hvilket ligeledes på sigt burde sikre en strategisk gevinst i forhold til potentialerne i øget datadeling og samarbejde på tværs af den offentlige sektor.

Det er imidlertid vanskeligt at identificere og beregne økonomiske gevinster for et målbillede, som vedrører forhold, som er af den særlige karakter, der er tale om i denne sammenhæng. Samtykker og frabedelser som retsgrundlag er blot et lille element, der indgår som en forudsætning i en lang række processer, som i realiteten handler om noget helt andet i form af databehandling/datadeling, sagsbehandling og behandling af personer inden for sundhedsdomænet.

Fælles tekniske infrastrukturløsninger vil dels kunne understøtte sammenhæng og vil dels i nogen grad kunne afløse behovet for lokale løsninger, men samtidig vil der være omkostninger forbundet med udvikling, tilpasning og tilslutning af lokale løsninger (fagsystemer, selvbetjeningsløsninger og domænespecifik infrastruktur). Desuden er det svært at opgøre gevinster, der først vil kunne høstes længere nede ad banen efter implementering, og som vil afhænge meget af graden af udbredelse, som igen er afhængig af scope og politiske beslutninger.

I dette afsnit gives der derfor kun en overordnet skitse af den overordnede værdiskabelse, som er mulige og kan forventes. Fokus er på kvalitative gevinster. Målbilledet fokuserer på de grundlæggende, infrastrukturelle forhold og kapabiliteter, hvorfor det er meget svært at sige noget meningsfyldt om de forretningsmæssige muligheder for økonomiske gevinster, som typisk vil være afhængige af konkrete behov og forhold i de enkelte forretningsdomæner.

Borgere

1. Borgerne kan få en bedre oplevelse af transparens, og at de er informeret, inkluderet og i kontrol med deres egne data.
2. Borgere kan få en bedre indsigt i og oplevelse af, at deres samtykker og frabedelser anvendes og respekteres.
3. Borgere kan få en mere tydelig oplevelse af en helhedsorienteret service fra det offentlige, hvor borgeren sættes i centrum.
4. Borgere kan lettere få mulighed for at opleve en ensartet og sammenhængende digital brugerrejse ved afgivelse af samtykke/frabedelse.
5. Borgere kan bedre opleve, at de digitale løsninger er brugervenlige og indgår i tværgående forløb, hvor samtykke kan gives til offentlige myndigheder på tværs af den offentlige sektor - og hvor relevant til private aktører.
6. Borgere kan i øget omfang og på en ensartet måde give digitalt samtykke til sagsbehandling, behandlingsforløb samt indhentning og videregivelse af persondata.
7. Borgere kan, hvor det er relevant, vælge en digital frabedelse i form af en privatmarkering eller en spærring
8. Borgere kan få et enkelt og samlet digitalt overblik over samtykker og frabedelser og kan, hvor det er relevant, få mulighed for nemt at ændre og tilbagekalde dem samt mulighed for at se hvilke organisationer, der tilgår dem.
9. De mange forskellige borgervendte digitale løsninger kan lettere tilpasses ud fra fælles rammer, så de understøtter tidssvarende brugsmønstre og behov, fx mobile platforme.
10. Borgere kan få notifikation om muligheden for at vedligeholde deres samtykker og frabedelser.
11. Borgere kan, hvor det er relevant og ud fra altruistiske hensyn tillade, at deres data som udgangspunkt kan anvendes til (udvalgte) forskningsprojekter og lignende.

12. Borgerne kan tilgå vejledninger om anvendelse af samtykke og frabedelse, og have mulighed for brug af både digitale og analoge kanaler, adgang til hjælp og support.

Organisationer og deres medarbejdere

13. Organisationer kan lettere demonstrere efterlevelse af lovgivningen.
14. Organisationer og domæner skal ikke genopfinde den dybe tallerken igen og igen, når der er fælles arkitektur, standarder og løsninger, som ligeledes sikrer ensartethed og genbrugelighed på tværs.
15. Medarbejdere og organisationer kan opleve, at administration af samtykke og frabedelse er digital, simpel, automatiseret og lettilgængelig og kræver få ressourcer.
16. Medarbejdere kan opleve, at indhentning, registrering, fremsøgning, adgangsstyring og anvendelse af digitale og analoge samtykker er nemt, sammenhængende, sikkert og effektivt.
17. Organisationer kan automatisere adgangsstyring understøttet af digitale samtykker og frabedelser.
18. Organisationer kan sikre, at kun rette fagpersoner har kendskab til den enkelte samtykke eller frabedelse.
19. Organisationer og deres medarbejdere kan tilgå vejledninger om anvendelse af samtykke og frabedelse, så myndighederne har den fornødne indsigt til at kunne anvende analoge og digitale samtykker på ensartet vis.
20. Organisationer og deres medarbejdere kan opleve, at det er nemt informere borgerne og eventuelle bisiddere om formålet, rettigheder og konsekvenserne ved et samtykke eller en frabedelse.

I det videre arbejde skal der ske en nærmere analyse af mulighederne for konkret værdiskabelse gennem inddragelse af relevante brugere, herunder både digitale og ikke-digitale borgere og medarbejdere i anvender-organisationer.

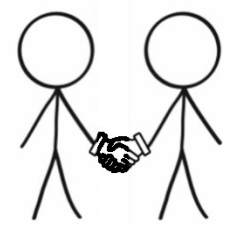
2. Strategi

Digital håndtering af samtykker og frabedelser kan betragtes som en katalysator for en sammenhængende offentlig sektor med borgeren i centrum, idet de kan understøtte datadeling, tværgående sagsbehandling og automatisering.

Sammenhængende håndtering af samtykke og frabedelse skal understøtte bedre kvalitet i samspillet mellem borgere og myndigheder. Den bedre kvalitet skal opnås gennem en mere ensartet håndtering af samtykker og frabedelser, understøttelse af processer på tværs af domæner og genbrug af data gennem datadeling.

Vision

Den fællesoffentlige vision for digitalt samtykke og frabedelse er:



Vision

Samtykke og frabedelse håndteres digitalt på en sammenhængende, tidstro og sikker måde, som er let at anvende og forstå for alle involverede.

Den mere detaljerede betydning af udvalgte nøgleord og formuleringer i visionen er forklaret i det følgende:

Samtykke og frabedelse er de to grundlæggende begreber, som dette målbillede drejer sig om. Begge disse begreber er vigtige til at afgøre, hvilken hjemmel der er til en given handling, fx i form af databehandling og udveksling af data.

Med *håndteres digitalt* menes, at samtykker og frabedelser registreres digitalt – også papirbaserede og mundtlige, hvor det giver mening og værdi. Det betyder, at en borger som hovedprincip skal afgive et samtykke eller en frabedelse digitalt. Hvis det ikke er muligt, fx for en ikke-digital borger, skal der være klare retningslinjer i et domæne for, hvordan man kan få hjælp til at give et mundtligt eller skriftligt samtykke, som - hvor det er relevant - kan registreres og attesteres digitalt af en medarbejder eller gives via en partsrepræsentant ved hjælp af en fuldmagt.

Med *sammenhængende* menes, at alle samtykker og frabedelser dannes ud fra fælles standarder og kan deles og anvendes til procesunderstøttelse i relevante it-systemer på tværs af den offentlige og den private sektor. Det betyder, at de - hvor det er relevant - kan deles og anvendes på tværs af domæner, sektorer, organisationer og it-systemer. Deling bør ske med inddragelse af borgeren gennem selve afgivelsen af samtykket, og konkret information om den påtænkte anvendelse skal således være understøttet af den skabelon, der lægges til grund for samtykket eller frabedelsen.

Med *tidstro* menes, at et registreret, ændret eller tilbagetrukket samtykke eller frabedelse slår igennem umiddelbart derefter hos alle relevante aktører. Ændringer i status kommunikeres fra datakilden i nærrealtid, så alle anvendere altid kan agere på et autoritativt grundlag, der er opdateret og validt.

Med *sikker* menes, at håndteringen af samtykker og frabedelser sker sikkert og på et ensartet niveau uanset i hvilken organisation, det sker. Niveauet defineres i relevante domæner og dokumenteres i skabelonerne for digitale samtykker og frabedelser. Borgerne skal føle sig

trygge ved, at deres samtykker og frabedelser respekteres. En fælles sikkerhedsmodel skal følges af alle aktører og it-systemer, så det er klart, hvem der har adgang til et samtykke eller en frabedelse, og hvilke rettigheder aktørerne har.

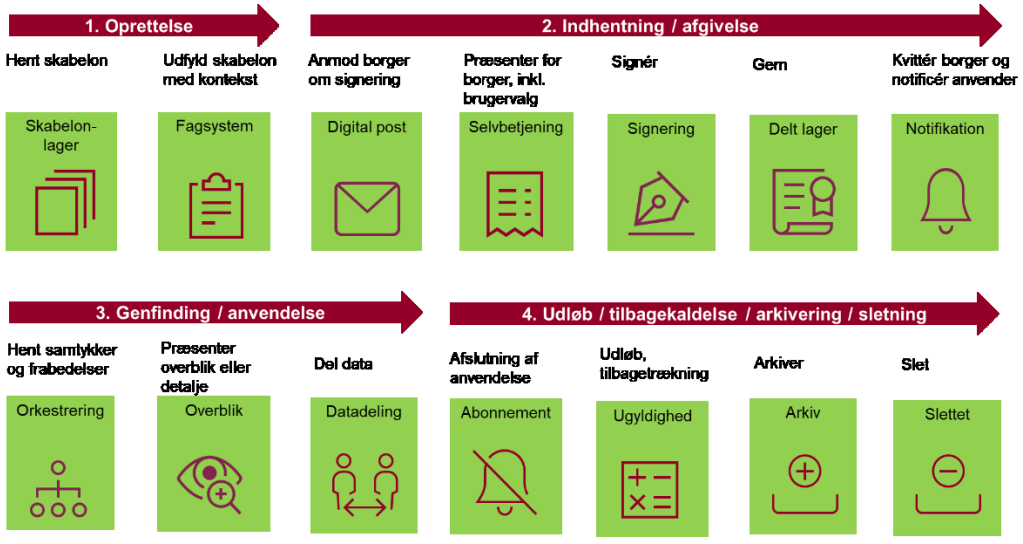
Med *let at anvende og forstå* menes, at det skal være let for digitale borgere at registrere, få overblik over, administrere og tilbagetrække samtykker og frabedelser og at forstå konsekvenserne heraf. Tilsvarende skal det være let for medarbejdere at få overblik over relevante samtykker og frabedelser, så de kan agere i overensstemmelse med dem. Desuden skal det være muligt at sætte et fagsystem op, så det understøtter automatisering af processer mest muligt ved at udnytte struktureret data fra et samtykke eller en frabedelse.

Med *alle involverede* menes alle de aktører, som skal håndtere samtykker og frabedelser digitalt og anvende de it-systemer, de håndteres i. Det omfatter borgere såvel som medarbejdere hos myndigheder og virksomheder.

Processer og funktioner i et livscyklusperspektiv

De mest centrale funktionelle behov er beskrevet i nedenstående figur (figur 2.1), som viser fire hovedprocesser, som favner den samlede livscyklus for et samtykke: 1) Oprettelse, 2) Indhentning / afgivelse, 3) Genfinding / anvendelse samt 4) Udløb / tilbagekaldelse / arkivering / sletning. En tilsvarende proces for frabedelse vil indeholde mange af de samme elementer med den væsentlige forskel, at det typisk er borgeren selv, der initierer processen.

Disse fire processer indebærer en række funktioner, som skal understøttes af de involverede it-systemer. Nogle funktioner skal fx håndteres af fagsystemer, andre af borgervendte løsninger, som fx selvbetjeningsløsninger, og atter andre af underliggende infrastruktur. Samlet set vil den samlede realisering af visionen påvirke en lang række digitale løsninger, der skal virke sammenhængende.



Figur 2.1 Ønsket proces for håndtering af samtykke/frabedelse gennem hele livscyklussen

Bemærk, at figuren ikke beskriver processer og funktioner knyttet til brugerstyring eller til den konkrete opgaveløsning, hvor samtykker og frabedelser bringes i anvendelse, herunder eksempelvis automatisering af forretningsprocesser og datadeling. Fx kan det i én proces være relevant for en medarbejder at se et overblik over samtykker knyttet til en sag og tilgå

detaljer, mens det i en anden proces kan håndteres automatisk af fagsystemet, uden at medarbejderen behøver at se eller gøre noget.

De overordnede mål og strategiske kapabiliteter, som beskrives i næste afsnit, udgør grundlaget for den nærmere definition af de processer og funktioner, der skal understøttes.

Mål og kapabiliteter

Den fællesoffentlige vision for samtykke digitalt realiseres gennem en række overordnede mål og understøttende kapabiliteter. Kapabiliteter handler om at være kapabel, i stand til noget og er med andre ord nogle overordnede evner, som skal understøttes organisatorisk eller teknisk.

Oprettelse

Mål: Der skal være klare juridiske rammer for krav til samtykke og frabedelse.

Kapabiliteter:

- Evnen til at håndtere samtykker digitalt på relevant lovgrundlag
- Evnen til at danne samtykker på basis af en lovmedholdelig skabelon.

Rationale: Det er en forudsætning for, at de enkelte myndigheder kan anvende samtykker og frabedelser efter fælles standarder, og at de juridiske rammer er nemme at fortolke i forhold til standarderne. Tilsvarende er det vigtigt, at der er klar governance omkring skabeloner.

Indhentning/afgivelse

Mål: Det skal være nemt at indhente/afgive, tilpasse, gemme og signere et samtykke eller en frabedelse.

Kapabiliteter:

- Evnen til at kommunikere indhold og konsekvenser af et samtykke eller en frabedelse
- Evnen til at håndtere relevante til- og fravalg i forbindelse med et samtykke eller en frabedelse
- Evnen til at håndtere digital signering eller attestation, også når der er flere, der skal signere et samtykke
- Evnen til at delegere afgivelse af samtykke og frabedelse via fuldmagt
- Evnen til at registrere, lagre og dele eksisterende og analoge samtykker og frabedelser digitalt uden ekstra besvær for borgeren.

Rationale: Det er en forudsætning for, at borgere, virksomheder og medarbejdere har en god brugeroplevelse, at det er nemt og trygt at indhente og afgive samtykke og frabedelse, og at alle relevante funktioner er tilgængelige og nemme at anvende. Alle relevante oplysninger skal gives på en måde, som er overskuelig, så det er let at forstå konsekvenserne af det afgivne samtykke eller frabedelse. Det gælder også, når en medarbejder fx skal registrere og attestere et mundtligt afgivet samtykke.

Genfinding / anvendelse

Mål: Der skal kunne dannes et tværgående og tidstro overblik over relevante samtykker og frabedelser og deres gyldighed.

Kapabiliteter:

- Evnen til at dele samtykker og frabedelser på tværs af organisationer og it-systemer
- Evnen til at fremsøge samtykker og frabedelser, der modsvarer behov for opgaveløsning på baggrund af strukturerede metadata om genstandsfelt, herunder for samtykker og frabedelser der har en indbyrdes relation
- Evnen til at levere data til et tværgående, borgervendt overblik over samtykker og frabedelser
- Evnen til at håndtere opdatering og notificere ved statusændringer af et samtykke eller en frabedelse
- Evnen til at registrere anvendelsen af et samtykke eller en frabedelse.

Rationale: Det er en forudsætning for en nem og tryg anvendelse, at såvel borgere som medarbejdere kan genfinde, dele og få et overblik over relevante samtykker og frabedelser på tværs af de offentlige myndigheder, fx i forhold til et sammenhængende behandlingsforløb. Borgeren skal kunne få et overblik over afgivne samtykker og frabedelser, om de er gældende, og hvilke organisationer der anvender dem, og det skal være nemt at kunne trække et samtykke eller en frabedelse tilbage, hvis det er relevant. Fagsystemet skal kunne håndtere forhold, der understøtter medarbejdernes arbejde, herunder at give overblik over om der er givet samtykke, ønskes privatmarkering eller ved evt. spærring sikre, at en given medarbejder ikke får adgang til følsomme data. Og man skal kunne få en tidstro besked ved ændring af status og gyldighed, så anvendelsen er lovmedholdelig fx i forbindelse med datadeling og sagsbehandling. Det skal være muligt at danne et overblik over, hvilke organisationer / systemer der har tilgået et givent samtykke eller en frabedelse på et delt lager. Desuden skal man lokalt kunne registrere anvendelsen af dette i en given forretningskontekst, så det er muligt at levere information om denne anvendelse til relevante formål, eksempelvis loginformation til borgerne på områder, hvor der er behov og den fornødne modenhed.

Udløb og tilbagekaldelse

Mål: Det skal være nemt at tilbagekalde et samtykke eller en frabedelse med en letforståelig beskrivelse af konsekvenser.

Kapabiliteter:

- Evnen til at håndtere udløb, arkivering og sletning af et samtykke gennem eksekvering af veldefinerede forretningsregler
- Evnen til at håndtere tilbagekaldelse af et samtykke eller en frabedelse end-to-end på baggrund af notifikation fra lager om statusskift.

Rationale: Et samtykke har en gyldighedsperiode, der kan være defineret på forskellige måder afhængig af domænespecifikke forhold. Det er forudsætning for en lovmedholdelig administration, at der er styr på udløb, og at dette får konsekvens ind i de processer og systemer, der anvender et samtykke. Ligeledes skal der være styr på krav til arkivering og sletning af samtykker og frabedelser. Det er en forudsætning for, at et samtykke er frivilligt, at det også kan fortrydes og trækkes tilbage lige så nemt, som det var at afgive. Hvis det skal ske, skal det være klart for borgeren, hvad konsekvenserne er. Tilsvarende skal det være let at annullere en frabedelse, men også her skal borgeren tydeligt orienteres om konsekvenserne. Og tilbagetrækningen skal slå igennem i anvendende systemer.

Brugerstyring

Mål: Brugerstyring og sikkerhed i de involverede it-systemer skal være transparent, utvetydig og velproportioneret.

Kapabiliteter:

- Evnen til at håndtere adgangskontrol på system-/organisationsniveau til delte samtykker og frabedelser på et delt lager
- Evnen til at håndtere brugerstyring på slutbrugerniveau lokalt og i domæner på tværs af involverede anvendersystemer på baggrund af opmærkning af samtykker og frabedelser
- Evnen til at begrænse deling af data via frabedelse i domæner, hvor dette er en borgerret.

Rationale: Målet er både at samtykker og frabedelser i sig selv skal kunne deles, og at de kan anvendes til at styre deling af andre data. Brugerstyringen skal tage hensyn til, at samtykker i sig selv kan være følsomme data. Det er en forudsætning for, at myndigheder og virksomheder kan deltage i deling af persondata, herunder deling af samtykker og frabedelser, at de har styr på kontrol af brugere, rettigheder og sikkerhed. Det betyder bl.a., at de skal overholde en fælles sikkerhedsmodel og relevant fællesoffentlig digital arkitektur og standarder. I domæner, hvor det er en borgerret at kunne lave en frabedelse i form af en privatmarkering eller spærring, skal dette være muligt på tværs af alle involverede organisationer og systemer.

Automatisering

Mål: Det skal være muligt at automatisere processer med understøttelse af digitale samtykker og frabedelser.

Kapabiliteter:

- Evnen til at kunne maskinfortolke samtykker og frabedelser semantisk
- Evnen til at automatisere processer og at behandle og dele data automatisk via anvendelse af digitalt samtykke og frabedelse.

Rationale: Det er en forudsætning for automatisering, at digitale samtykker og frabedelser kan udformes, så de kan understøtte automatisk maskinfortolkning. Det kan fx være ved brug af data, som i et standardiseret format beskriver et samtykkes anvendelsesformål, aktører der må anvende det som hjemmel, data der må deles og rammer for samtykkets gyldighedsperiode. Disse data kan kobles til automatisk fortolkning af forretningsregler, således at man kan automatisere en række forskellige funktioner og arbejdsgange. Ved at

anvende fælles standarder kan denne automatisering ske på tværs af organisationer og it-systemer.

Principper

I dette afsnit gennemgås en række principper, som skal være styrende dels for det fællesoffentlige projekts leverancer i form af arkitektur, specifikationer og løsningskomponenter og services dels for tilsvarende leverancer på domæneniveau samt for de offentlige og private forretnings- og it-løsninger, som kobles til den samlede løsning.

Der er taget udgangspunkt i de fællesoffentlige arkitekturprincipper fra hvidbogen om digital arkitektur, og principperne er organiseret ud fra de otte FDA-grundperspektiver på den digitale arkitektur.

Hvidbogens principper uddybes her med formuleringer af implikationer, som er direkte relateret til emnet 'samtykke og frabedelse'.

1. Arkitektur styres på rette niveau efter fælles rammer

    - Håndtering af samtykke og frabedelse baseres på fælles grundlæggende arkitektur og specifikationer underlagt national governance.
    - Domænefællesskaber kan aftale domænespecifikke anvendelsesprofiler, og skabeloner for samtykker og frabedelser baseres på fælles grundlæggende specifikationer.
    - Håndtering af samtykke og frabedelse i domæner giver de enkelte parter tilpas frihedsgrad til, at de kan overholde deres egne interne retningslinjer og processer.

2. Arkitektur fremmer sammenhæng, innovation og effektivitet

    - Det er nemt for borgere at administrere (afgive, få overblik og trække tilbage) samtykke og frabedelse på tværs af organisationer og it-systemer.
    - Det er nemt for organisationer og deres medarbejdere at administrere (indhente, dele og anvende) samtykker og frabedelser på tværs af organisationer og it-systemer.
    - Håndtering af samtykke og frabedelse på tværs af den offentlige sektor realiseres gradvist og behovsstyret med fokus på levering af nytteværdi.
    - Nye løsninger afprøves på forretningsniveau og teknisk gennem dialog og pilotafprøvning, inden applikations- og teknologiunderstøttelse for samme udformes endeligt og udrulles bredt.
    - Nationale tiltag til håndtering af samtykke og frabedelser udformes i bedst mulig overensstemmelse med internationale standarder og bedste praksis.
    - Der anvendes modne bredt understøttede teknologier til at højne leverandøruafhængighed og fortrinsvis driftsmodnede løsningskomponenter med gode referencer fra eksisterende anvendelser.
    - Lokale komponenter til håndtering af samtykke og frabedelse koordineres med henblik på genbrug af såvel nye som allerede etablerede løsningselementer.

3. Arkitektur og regulering understøtter hinanden

    - Den grundlæggende arkitektur og standarder tager så vidt muligt højde for juridiske bindinger gennem indarbejdelse af begreber og krav og gennem rummelighed i forhold til forskellighed i lovgivning.

- Samtykke og frabedelser baseres på skabeloner, der kan sikre lovmedholdelighed.
- Den organisation, der indhenter et samtykke eller registrerer en frabedelse, har ansvar for, at relevant lovgivnings forskellige bestemmelser følges.
- Hvis der er identificeret uhensigtsmæssige juridiske bindinger i forhold til at anvende samtykke og frabedelser, vil projekter kunne bidrage til udarbejdelse af forslag til love og regler.

4. Sikkerhed, privatliv og tillid sikres

- Alle aktører i det digitale økosystem følger en fælles sikkerhedsmodel og rammer for ansvaret for brugerstyring og adgangskontrol.
- Ansvaret for den konkrete anvendelse, herunder lokal brugerstyring, påhviler den organisation, der anvender den enkelte samtykke og frabedelse.
- Den tværgående infrastrukturs understøtter håndhævelsen af dette ansvar på organisations- og systemniveau, men den kan ikke i sig selv sikre håndhævelsen lokalt og i domæner på enkeltbrugerniveau.

5. Processer optimeres på tværs

- Det er nemt at oprette og administrere et samtykke eller en frabedelse på grundlag af en skabelon, som er lovmedholdelig og overholder relevante krav.
- Afgivelsen af samtykke og frabedelse er frivillig, og hvor det er relevant, er det muligt at foretage til- og fravalg eller trække tilbage.
- Konsekvensen af at afgive, ikke at afgive en viljestilkendegivelse eller trække denne tilbage præsenteres klart og letforståeligt for borgeren.

6. Gode data deles og genbruges

- Samtykke og frabedelser opsamles én gang og anvendes i alle relevante sammenhænge i overensstemmelse med gældende regler.
- Tværgående håndtering af samtykke og frabedelser forudsætter en fælles datamodel og udvekslingsformat baseret på fælles begrebsforståelse.
- Informationsmodellen, der udtrykker mulighederne for omfanget af samtykker og frabedelser, skal være så fleksibel, at den kan rumme fremtidige ændringer.
- Indholdet af og konsekvenser ved samtykke og frabedelser er forståeligt for dem, der afgiver og anvender dem.
- Borgeren behøver ikke detaljeret kendskab til organisation og it-systemer for at kunne afgive og administrere sine samtykker og frabedelser.
- Medarbejderen skal være klædt på med relevant viden og kompetencer til at kunne håndtere digitale samtykker og frabedelser
- Et samtykkes og frabedelses validitet og status er klar og tydelig for dem, der skal anvende det/den.

7. It-løsninger samarbejder effektivt

- Applikationer og komponenter til håndtering af samtykke og frabedelse i et domæne kan indgå i de fælles løsninger i det enkelte domæne og i de tværgående løsninger som fx borgervendt overblik.

8. Data og services leveres driftssikkert

- Fælles komponenter og delte lagre stiller åbne API'er til rådighed og overholder aftalte SLA'er.

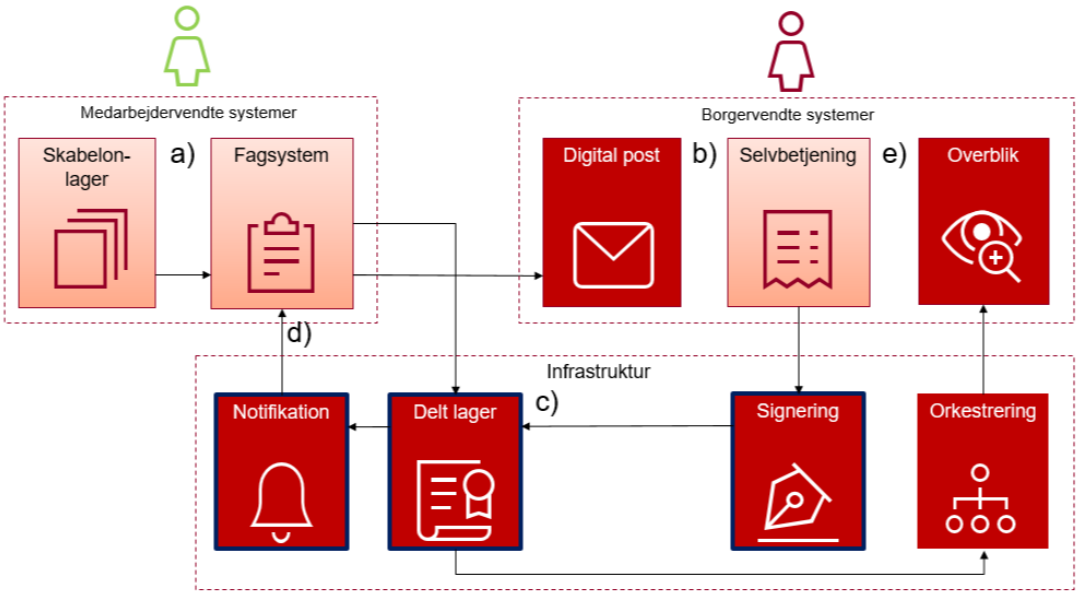
Teknisk arkitektur: Sammenhængende komponentlandskab

For at etablere sammenhængende digitale løsninger, hvor man kan dele samtykker og frabedelser, er der en række komponenter, som skal kunne arbejde sammen som et digitalt økosystem, hvor fagsystemer og selvbetjeningsløsninger understøttes af en sammenhængende infrastruktur.

Nedenstående figur (

figur 2.2) viser de mest centrale komponenter på logisk niveau, hvilket betyder, at der kan være flere instanser af de enkelte komponenter. Fx vil der være mange fagsystemer og selvbetjeningsløsninger, ligesom der kan være flere lagre og portaler til visning af overblik. De mørkerøde komponenter er fællesoffentlige, mens de lyserøde typisk drives af en myndighed eller et domænefællesskab. De øverste komponenter er brugervendte, mens de nederste er fælles underliggende infrastruktur.

Et samtykke eller en frabedelse dannes på baggrund af en formaliseret skabelon, der hentes på et skabelonlager. Det kan enten dannes via et fagsystem eller via en selvbetjeningsløsning: a) En medarbejder danner via fagsystemet en digital postmeddelelse med anmodning om samtykke, som leder borgeren til en selvbetjeningsløsning, hvor samtykke kan afgives, eller b) borgeren initierer selv processen via en selvbetjeningsløsning. c) I begge tilfælde lagres samtykket/frabedelse på et delt lager, og signering sker via en service fra en central signeringskomponent. d) Når samtykket er signeret, får medarbejderen besked via fagsystemet, der får en notifikation fra samtykkelageret. e) Borgeren kan tilgå et overblik over samtykker på en fælles overbliksløsning som fx borger.dk eller sundhed.dk eller anden relevant lokal eller domænespecifik portalløsning, der henter samtykker og frabedelser fra delte lagre via den fællesoffentlige orkestreringskomponent.



Figur 2.2 - Oprettelse af samtykke/frabedelse i fælles digitalt økosystem

I ovenstående figur er de tre centrale komponenter, som indgår i en MVP-løsning fremhævet med fed ramme i ovenstående figur. Det drejer sig om:

- En **lagerkomponent** hvor fagsystem eller selvbetjeningsløsning kan lagre og læse samtykker og frabedelser
- En **signeringskomponent** som kan præsentere et samtykke for borgeren til signering
- En **notifikationskomponent** som kan give besked til fx et fagsystem, når der sker en status ændring i et samytykke eller en frabedelse.

Ud over disse tre centrale komponenter indgår der i det samlede målbillede en række yderligere komponenter.

Der er identificeret et muligt behov for to *midlertidige støttekomponenter*, der har til formål at understøtte, at organisationer nemt kan komme i gang med at deltage i løsningen, uden at man nødvendigvis skal have fx et fagsystem tilpasset: En **registreringskomponent** skal understøtte indlæsning af samtykker og frabedelser på det delte lager manuelt eller automatisk fx med brug af en softwarerobot (RPA). Det kan fx dække både eksisterende og nye samtykker, der dannes i egne systemer og analoge samtykker. En **fremsøgningskomponent** skal understøtte fremsøgning og visning af samtykker og frabedelser fra lageret, herunder mulighed for at abonnere på hændelser, fx når et samtykke skifter status ved signering.

Desuden indgår der en række komponenter, som fungerer som støttefunktioner, herunder en **hjemmeside** med relevante retningslinjer, standarder (datamodeller, klassifikationer, snitfaldebeskrivelser mv.), tilslutningsvejledning, driftsinformation mv. vendt mod organisationer og leverandører i forhold til tilslutning og drift. Hertil kommer eventuelt på sigt fælles **kataloger** over datamodeller og forretningsregler til at understøtte automatisering af datadeling, brugerstyring mv. Tilsvarende kan der være behov for et **indeks**, hvis der etableres mange sådanne delte lagre.

For at understøtte udbredelse skal der etableres passende **testsystemer**, som kan understøtte den lokale udvikling, implementering og drift. Der skal tillige være en **supportfunktion for professionelle anvendere**, der kan håndtere spørgsmål og behov for hjælp i forhold til fx udvikling og vedligehold af skabeloner, forretningsmæssig implementering med tilpasning af processer og forretningsgange og uddannelse af medarbejdere samt støtte til teknisk udvikling, implementering og drift.

Sidst, men ikke mindst, skal der være relevante **brugerstyringskomponenter** koblet til alle komponenter, som skal sikre, at alle løsninger understøtter den fælles, tværgående sikkerhedsmodel. Et højt niveau af sikkerhed stiller krav til sikkerheden på tværs af alle komponenter i økosystemet. Evnen til at levere sikker og effektiv brugerstyring er derfor også afgørende på det niveau for automatisering af processer og datadeling, der realiseres på et givent tidspunkt og på et givent anvendelsesområde.

Endelig skal det bemærkes, at der vil være behov for en **digital og analog supportfunktion for slutbrugere** vendt mod borgere og medarbejdere i virksomheder.

Realisering af målbilledet

Dette afsnit beskriver en overordnet tilgang til realisering af det fælles målbillede.

Grundscenarier og anbefalet tilgang

Her beskrives to grundscenarier med det formål at sætte den overordnede scene for beskrivelsen af en strategi for realisering og migrering.

Et **big-bang scenarium,** hvor visionen realiseres på et bestemt tidspunkt, hvor alle forudsætninger skal være på plads.

- Dette scenarie forudsætter en konsolideret fælles arkitektur, standarder og infrastruktur suppleret med en styringsmæssig ramme, som kan gennemtvinge et stærkt politisk mandat med obligatoriske krav til de relevante aktører, som skal deltage i økosystemet.
- Dette scenarium vil kunne afføde ekstra store decentrale omkostninger i forbindelse med tilpasninger og tilslutning til økosystemet, hvis der ikke tages hensyn til naturlig modning og gældende kadencer for genudbud af fagsystemer og domæneinfrastruktur i de forskellige domæner.
- Det vil endvidere lægge et meget stort pres med store krav til organisatorisk modning og styring. Der er stor risiko for, at det vil tage lang tid at forberede et "big bang".

Et **iterativt scenarium,** hvor målbilledet realiseres over tid med udgangspunkt i første versioner af fælles arkitektur, standarder og en initial MVP-løsning, som løbende kan udvides med nødvendig og efterspurgt funktionalitet over en årrække.

- Dette scenarie gør det muligt at komme hurtigt i gang. Tværgående anvendelse af samtykker kan ske, når alle relevante aktører er med i forhold til en konkret anvendelse.
- Borgerne og organisationer/medarbejdere vil ikke få det ønskede overblik i de første faser, men stadig skulle forholde sig til fragmenterede løsninger.
- Dette scenarie indebærer en risiko for, at early movers kommer til at sætte dagsordenen, samtidig med at der kan være en risiko for, at de løbende skal vedligeholde og videreudvikle i takt med, at andre kommer med, hvis det giver anledning til nye krav og standarder.

Det anbefales, at realiseringen af vision og mål sker gradvist med udgangspunkt i det iterative scenarie med henblik på at kunne påbegynde arbejdet med at indfri den overordnede vision for digitalt samtykke og frabedelse inden for en overskuelig tidshorisont samt behovet for større modning inden for en række underområder og temaer.

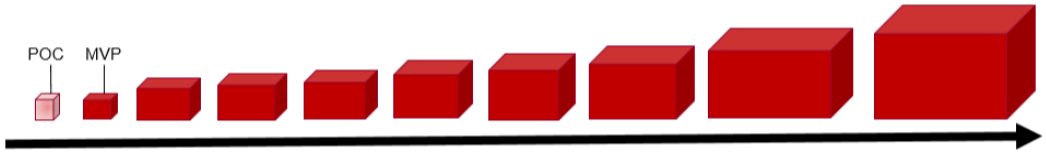
Den gradvise udvikling vil ske i en række dimensioner, herunder:

- Domæner der omfattes (afklaring og aftaler)
- Kapabiliteter der understøttes (udvikling af funktioner og data)
- Systemer der tilsluttes (implementering og idriftsættelse)

De tre dimensioner kan realiseres parallelt og asynkront, så der fx er løsninger i nogle domæner, der understøtter få kapabiliteter, mens andre understøtte flere.

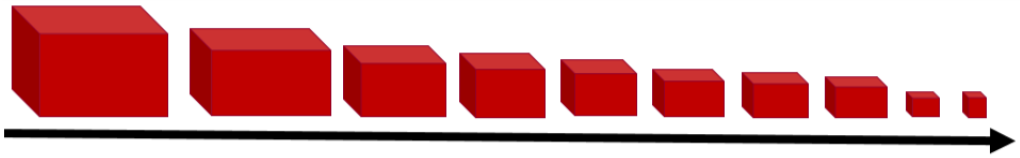
Nedenstående figur (

figur 2.3) giver en abstrakt illustration af en mulig proces for migrering på systemniveau.



Figur 2.3 - Abstrakt illustration af en mulig proces for udrulning i de tre dimensioner områder, kapabiliteter og systemer

Nedenstående figur (Figur 2.4 Abstrakt illustration af muligt faldende barrierer og omkostninger i forbindelse med udbredelse og implementeringFigur 2.4) illustrerer, hvordan der over tid kan forventes at være faldende omkostninger forbundet med implementering på et givent område, i og med at der løbende sker en afklaring og opbygning af viden, kompetencer, udvikling af genbrugelige anvendelsesprofiler og skabeloner og tilpasning af infrastruktur og fagsystemer. Dette vil alt andet lige gøre det nemmere, hurtigere og billigere at få nye områder med ind i økosystemet.



Figur 2.4 Abstrakt illustration af muligt faldende barrierer og omkostninger i forbindelse med udbredelse og implementering

Initial realisering af de centrale kapabiliteter (MVP)

Den initiale realisering af de centrale kapabiliteter skal ske gennem udvikling af komponenter og services efter en MVP-tilgang. Det vil sige, at der i første omgang fokuseres på at udvikle de centrale komponenter og services, således at disse kan implementeres og afprøves på udvalgte områder. Til gengæld er det vigtigt, at de første områder repræsenterer strategisk nøgleaktører og omfatter infrastruktur, fagsystemer og selvbetjeningsløsninger, som kan bidrage optimalt til teknisk og forretningsmæssig modning.

MVP-løsningen skal først og fremmest understøtte mål om evnen til at oprette og indhente et samtykke eller frabedelse, der er signeret og lagret på et delt lager. Dette omfatter både analoge og digitalt fødte samtykker og frabedelser, der ved at anvende skabeloner, kan beriges med metadata, så de kan deles via infrastrukturen.

Desuden skal MVP understøtte evnen til at fremsøge delte samtykker og frabedelser og give medarbejdere og borgere overblik over relevante samtykker og frabedelser, herunder simpel søgning, overbliksvisning og mulighed for at abonnere på hændelser, således at en medarbejder fx kan få advis, når eksempelvis et samtykke er afgivet eller trukket tilbage af en borger. Derfor skal MVP-løsningen konkret omfatte:

- En lagerkomponent, med et API, så man kan gemme og finde samtykker og frabedelser
- En signeringskomponent med et API, så man kan hente et samtykke eller en frabedelse til præsentation og signering

- En notifikationskomponent, så man kan opsætte et abonnement og få besked, når der sker ændringer i status på et samtykke eller en frabedelse

Nogle organisationer og deres medarbejdere vil kunne have udfordringer med at anvende og tilslutte egne systemer direkte til disse snitflader. For at hjælpe disse aktører til at anvende det fælles lager kan der udvikles såkaldte støttesystemer til registrering/lagring og til fremsøgning/visning af samtykker og frabedelser. Disse løsninger kan udvikles som open source komponenter, der enten kan implementeres centralt, i et domæne eller lokalt. Den konkrete løsning skal understøtte tilpasning til konkrete forretningsbehov, således, at man eksempelvis let kan registrere på basis af en domæneskabelon, og ansvaret for brugerstyring skal være klart forankret i domænet eller hos den enkelte organisation. Disse løsninger betragtes i udgangspunktet som optioner, der kan udvikles, hvis der viser sig et konkret behov.

- Støttesystem-Registrering: En komponent, der understøtter registrering på vegne af et eller flere fagsystemer, der ikke selv har kapabiliteten. Kan fx anvendes til at registrere eksisterende og analoge samtykker. Kan fx indrettes, så den kan anvendes manuelt eller automatisk via brug af et API eller en software-robot i en brugergrænseflade.
- Støttesystem-Fremsøgning: En komponent, der understøtter fremsøgning af samtykker og frabedelser på vegne af et eller flere fagsystemer, der ikke selv har kapabiliteten. Servicen skal understøtte fremsøgning fra et eller flere relevante lagre. Servicen kan fx indrettes, så den kan anvendes af en slutbruger, et fagsystem eller en softwarerobot.

Mit Overblik kan som del af borger.dkvise et borgervendt overblik over samtykker og frabedelser, som kan hentes fra et delt lager, som overholder fælles standarder. Digital Post vil fx kunne anvendes til at sende meddelelser til borgeren om, at der er et samtykke, som afventer godkendelse eller fornyelse. Derfor kan der i så fald tillige være behov for i samarbejde med Mit Overblik-projektet at udarbejde:

- En brugergrænseflade for visning af tværgående overblik over samtykker og frabedelser på borger.dk som del af Mit Overblik.
- En understøttelse af dette via tilpasning af den fællesoffentlige orkestreringskomponent med nyt dataområde og tilslutning af lager.

For at understøtte de forskellige aktører og leverandører, der skal udvikle løsninger og tilslutte sig infrastrukturen, er der behov for en generel kommunikation, vejledning og rådgivning samt muligheder for at gennemføre test af blandt andet semantisk, teknisk og sikkerhedsmæssig interoperabilitet. Som grundlag for dette er der derfor behov for

- En hjemmeside hvor man kan få adgang til al relevant dokumentation, som fx målbillede, referencearkitektur, sikkerhedsmodel, tekniske specifikationer som udvekslingsformat og API-specifikationer, genbrugelig kode mv.
- Et testmiljø med API'er til de påtænkte services og mulighed for at oploade og trække på testdata.

Den grundlæggende brugerstyring understøttes af sikkerhedsmodellen, som er beskrevet kort i kapitlet om sikkerhed nedenfor. Realiseringen kræver en konkretisering af sikkerhedsmodellen, bl.a. med aftaler om fælles udfaldsrum for opmærkning af hvilke aktører, der må tilgå et samtykke eller en frabedelse. Som led i MVP løsningen skal sikkerhedsmodellen som minimum understøttes af NemLogin og MitID.

Med hensyn til de strategiske mål vedrørende brugerstyring og automatisering på baggrund af strukturrede data i et samtykke er det pt. mere uklart, hvordan disse kapabiliteter vil blive realiseret. En mere avanceret automatisering af brugerstyringen og af datadeling i tværgående processer på basis af maskinfortolkning af samtykker og frabedelser afhænger i høj grad af de konkrete forretningsmæssige ambitioner i de enkelte domæner og myndigheder/organisationer. Det stiller fx store krav til håndteringen af brugerstyring på tværs af den centrale infrastruktur (fx NemLogin) og infrastrukturen i det pågældende domæne (fx KOMBIT adgangsstyring og kommunens lokale adgangsstyring). Desuden vil det kræve en modning af metoder til regelfortolkning og datamodeller, ligesom der kan blive behov for komponenter til at lagre, dele og håndtere regler og datamodeller, som overholder fælles specifikationer. Denne avancerede del vil ikke være del af MVP.

Initial afprøvning via pilotområder

Den initiale implementering på det forretningsmæssige niveau bør ske gennem en række pilotområder, som dels skal bidrage til at modne og kvalitetssikre indsatsområdet, herunder særligt den fælles arkitektur, specifikationer og infrastruktur, og den domænespecifikke implementering i form af bl.a. fælles domæneskabeloner og tilpasning af relevant infrastruktur, fagsystemer og borgervendte løsninger.

De udvalgte pilotimplementeringer bør dække både statslige, regionale og kommunale myndigheder såvel som private organisationer i form af fx forsyningsselskaber, privatpraktiserende læger eller andre tilsvarende typer af private aktører.

Foreløbige bud på kandidater til pilotområder er forsyningsområdet, sundhedsområdet og socialområdet. De enkelte pilotområders deltagelse, ambitionsniveau og implementeringsplaner aftales nærmere af de relevante interessenter.

Spørgsmål, der skal besvares via MVP og pilotafprøvning

Den samlede proces for realisering af målbilledet kan ses som tre hovedfaser:

1. **Forberedende fase** med fokus på foranalyse samt udarbejdelse af målbillede, referencearkitektur og grundlæggende specifikationer i form af fælles begreber, informationsmodel, datamodel, udvekslingsformat og sikkerhedsmodel
2. **Initial implementeringsfase** med fokus på udvikling af fælles services i en central MVP-løsning samt udarbejdelse af skabeloner, gennemførelse af tekniske og organisatoriske tilpasninger og implementering og afprøvning i udvalgte pilotprojekter inden for og på tværs af domæner, der repræsenterer væsentlige use cases og nøgleinteressenter.
3. **Udbredelsesfase** med fokus på afklaring af behov og barrierer, håndtering af disse gennem aftalte indsatser og eventuelle lovændringer samt aftaler om anvendelse og udbredelse.

Den initiale afprøvning kan derfor ses som en væsentlig bro mellem fase 1 og fase 3, hvor det er afgørende, at fase 2 besvarer en række centrale spørgsmål:

- Er det overordnede løsningskoncept og de udarbejdede arkitekturprodukter og specifikationer egnede til at understøtte de forretningsmål, som pilotprojektets interessenter har? Er der behov for at tilpasse nogle af disse arkitekturprodukter? Er der behov for at tilpasse målbilledet, dets ambitionsniveau og tilgang til udbredelse i fase 3?

- Har den udviklede MVP løsning de nødvendige funktioner og egenskaber til at kunne understøtte anvendernes forretningsbehov og brugerbehov på en måde, der er brugervenlig, effektiv og sikker?
- Har anvendelsen i pilotprojekterne tilført en værdi til myndighedernes forretning og borgerne? Eksempelvis ved at lette arbejdsgange, skabe større sikkerhed omkring håndtering af borgernes data eller ved at give borgerne bedre indsigt i, hvordan myndighederne håndterer deres data?
- Hvad tilsiger erfaringerne, at der skal til for, at den påtænkte løsning kan implementeres og give værdi i et domæne og lokalt i den enkelte organisation og den konkrete opgaveløsnings kontekst? Hvilke hensyn og aktiviteter bør der indtænkes i en fremadrettet planlægning af implementering og udbredelse på nye områder?

Decentrale opgaver i domæner og organisationer

Der lægges med dette målbillede op til en samlet løsning, hvor der er en generel infrastruktur, der understøtter mange forskellige forretningsbehov. Den fællesoffentlige MVP-løsning indgår i den generelle infrastruktur og skal derfor ses som en "smal" løsning i den forstand, at den ikke løser alle behov, men netop giver en fleksibilitet til, at man lokalt og i domæner kan understøtte forskellige behov med brug af fælles infrastruktur.

Det betyder, at en væsentlig del af arbejdet med specificering og implementering af de enkelte samtykker og frabedelser udlægges til domænerne og de enkelte organisationer. Et domæne kan fx være sundhedsområdet, socialområdet eller forsyningsområdet. Der er ikke en fast definition eller afgrænsning af et domæne, og der er en række situationer, hvor specificering og implementering skal ske på tværs af domæner, eksempelvis på tværs af sundheds- og socialområdet, eller som i tilfældet med helhedsorienteret indsats på tværs af socialområdet, beskæftigelsesområdet og uddannelsesområdet. Fx vil et samarbejde om behandling af patienter i hjemmet kræve tilpasninger på tværs af EPJ-systemer i sundhedssektoren og fagsystemer i kommunerne, herunder tilpasning af relateret infrastruktur.

En stor del af forretningslogikken og omkostningerne påhviler derfor de enkelte domæner og organisationer i form af implementering i infrastruktur, fagsystemer og selvbetjeningsløsninger. Dette er en omfattende og kompleks opgave, og det betyder, at de organisationer og domæner, der skal indgå i økosystemet, står over for store strategiske investeringer, såfremt man ønsker at strømline og gå ad den fællesoffentlige vej.

Der vil der være behov for at foretage tilpasninger i infrastruktur, fagsystemer og selvbetjeningsløsninger. I eksisterende løsninger vil dette indebære væsentlige ændringer. I nye systemer bør det indgå som en del af de grundlæggende krav. Desuden kan der være en række situationer, hvor man i den enkelte organisation eller i et domæne ønsker at anvende egne komponenter, fx til lagring, deling eller udstilling af viljestilkendegivelser. Det kan enten være gennem nyudvikling eller tilpasning af eksisterende løsninger.

I domænerne (eller på tværs af domæner) vil der være behov for en opbygning af en fælles governance inden for de forskellige domæner og i relevante tilfælde på tværs af domæner. I mange tilfælde vil der skulle skabes en styring på tværs af såvel stat, region og kommune såvel som på tværs af den offentlige sektor og private aktører.

- Inden for et domæne vil der være behov for at aftale en organisatorisk ramme og procedurer for udvikling af fælles specifikationer, herunder fastlæggelse af

anvendelsesprofiler for datamodeller og sikkerhedsmodeller, herunder relevante klassifikationer, udvikling og vedligehold af skabeloner samt udstilling af disse, fx via et delt skabelonlager.

- I tilfælde, hvor der skal laves fælles skabeloner og sikkerhedsmodeller på tværs af domæner og sektorer, vil der være behov for fælles aftaler om specificering og implementering. Fx skal der udarbejdes modeller for genstandsfelt og virkefelt samt en harmonisering/standardisering af disse. Dette understøttes af de fællesoffentlige støttefunktioner, der fremgår under afsnittet 'Teknisk arkitektur: Sammenhængende komponentlandskab'
- Denne styring bør også inddrage repræsentanter for borgerne såsom patient-/pårørendeforeninger.

De enkelte organisationer, der skal indhente og anvende samtykker og frabedelser, skal foretage sig en række ting, for at kunne blive en del af det tværgående fællesskab.

- Først og fremmest har de ansvaret for at foretage tilslutning og integration til de relevante services i de centrale komponenter eller tilsvarende services i domænespecifikke komponenter.
- Organisationer, der indhenter samtykker, skal sikre mekanismer til at anvende domæneskabeloner, og hvis det er relevant selv udvikle og vedligeholde skabeloner. Dette kan omfatte opgaver med specifikation af anvendelsesprofiler på den fællesoffentlige datamodel, fx med hensyn til valg af klassifikationer til beskrivelse af afgrænsninger af et samtykkes anvendelsesformål og sikkerhedsafgrænsning af, hvem der må tilgå og anvende et samtykke. Denne type opgaver skal udføres af specialister med viden om jura, sikkerhed, opgaver, semantik og teknik.
- Både organisationer, der indhenter, og organisationer, der alene anvender viljestilkendegivelser skal foretage de nødvendige lokale tilpasninger af eksisterende eller nye løsninger, så de kan overholde fælles specifikationer. Det omfatter fx lokal infrastruktur, fagsystemer og borgervendte løsninger.
- Eventuel nyudvikling af eksempelvis fagsystemer eller selvbetjeningsløsninger, der skal kunne indhente eller genbruge et samtykke bør anvende de kommende fællesoffentlige specifikationer som del af kravmaterialet.
- Endelig skal den enkelte organisation være opmærksom på, at der kan være behov for at sikre relevante tilpasninger af egen organisation, processer og kompetencer.

Videre arbejde med arkitektur, tekniske specifikationer og fælles retningslinjer

Parallelt med MVP'en er det planen at udarbejde en referencearkitektur, som skal fungere som byggevejledning. Denne laves i første omgang som grundlag for udvikling af MVP og implementering i de domæner, der skal være piloter for anvendelse. Det er forventningen, at den herefter skal konsolideres forud for en videre udbredelse i samfundet.

Desuden skal der aftales en fælles, tværgående sikkerhedsmodel og en række fælles, grundlæggende tekniske specifikationer herunder begrebs- informations- og datamodel samt udvekslingsformat. Disse skal danne grundlag for de skabeloner og anvendelsesprofiler, der skal udvikles og anvendes i de enkelte domæner. Disse skal ligeledes udvikles til at dække behov i forhold til MVP og piloter og det kan forventes, at disse også skal opdateres efterhånden som der gøres erfaringer, ligesom der kan arbejdes med udvikling af understøttelse af yderligere forretningsbehov.

Endelig skal det nævnes, at det danske arbejde så vidt muligt søges afstemt med beslægtet internationalt standardiseringsarbejde, herunder arbejde i regi af EU. Det er i den sammenhæng vigtigt at bemærke, at Danmark er på forkant med udviklingen, og at det danske arbejde har et bredere scope end det arbejde, der pågår internationalt, hvor fokus er på samtykke til databehandling, drevet af GDPR-forordningen. Særligt vil der i 2022 fra det danske arbejdes side være fokus på, om der i EU-regi peges på fælles specifikationer for samtykke i forbindelse med den kommende Datastyringsforordning.

Nedenstående figur (figur 2.5) illustrerer den overordnede proces for udvikling og konsolidering af fælles arkitektur, specifikationer og infrastrukturløsninger.

Figur 2.5 - Proces for udvikling og konsolidering

Der ligger desuden et betydeligt arbejde for de enkelte domæner. Der skal der for udarbejdes en overordnet tidsplan for udarbejdelse af målbilleder, arkitektur og anvendelsesprofiler på de tekniske specifikationer samt ikke mindst skabeloner i de enkelte domæner. Dette arbejde skal starte med en styringsaftale mellem relevante parter. Denne proces er beskrevet konceptuelt i nedenstående figur (figur 2.6).

Figur 2.6 - Proces for implementering i domæner

Proces for udbredelse

Der skal tilrettelægges **en fælles proces for udbredelse**, som løbende og efter aftale kan bidrage til at få nye områder ind i økosystemet ved at implementere relevante aftaler, skabeloner og tekniske specifikationer.

Processen skal sikre, at der efter aftale mellem de centrale interessenter sker en løbende afklaring af fælles tilgang til realisering på relevante områder. Som eksempler på områder kan nævnes sundhed, beskæftigelse, social, uddannelse, forsyning og ejendom. Den fælles tilgang skal fx kunne udmøntes i aftaler om fælles målbillede og plan for realisering af relevante aktører inden for et givent område. Som grundlag for dette bør der gennemføres områdeanalyser. Områdeanalyserne kan eksempelvis belyse:

- Borgervendte behov for at kunne afgive samtykke og frabedelse eller for at kunne ændre disse eller trække dem tilbage samt behov for overblik.
- Forretningsmæssige behov for deling af samtykker og frabedelser, deling af data og data om anvendelsen af samtykker eller frabedelser. Sidstnævnte omfatter fx behov for at anvende data om samtykker og frabedelser fra centrale lagre til sekundære formål, fx statistik og ledelsesinformation (anonymiseret).
- Eventuelle juridiske barrierer. Eventuelle behov for ændringer af lovgivning skal beskrives, således at de kan forelægges for relevant ressortministerium. I forbindelse med de juridiske afklaringer bør det undersøges, i hvilken grad data om samtykke og frabedelse kan deles med centrale myndigheder (til brug for fx løbende statistikbaseret opfølgning). Løsningen kan blandt andet være relevant for samtykkebaserede indsatser, hvor samtykket angiver en form for visitation.
- Modenhed og udfordringer samt eventuelle øvrige barrierer i forhold til jura, herunder fortolkning, samt udfordringer i forhold til sikkerhed, organisation, information, applikation og infrastruktur.
- Tilgang til teknisk realisering, herunder om der skal bygges eller tilpasses fælles infrastruktur i eller på tværs af domæner. Ligeledes bør det afklares, hvordan man skal arbejde med fælles sikkerhedsmodel, og med anvendelsesprofiler, skabeloner og klassifikationer inden for området.
- Eventulle behov for vejledninger, arkitekturprodukter eller lignende, som bør udarbejdes i regi af et domæne eller fællesoffentligt, skal tilsvarende beskrives, således at der kan udarbejdes et opdrag.
- Desuden bør den enkelte analyse – på et overordnet niveau – belyse forventede omkostninger, og muligheder fx i form af "windows of opportunity" i forbindelse med udvikling af nye it-systemer eller genudbud af fagsystemer.

På baggrund af områdeanalyserne kan der udarbejdes forslag til konkrete aftaler mellem relevante parter om udbredelse og anvendelse inden for et scope, der kan omfatte organisationer i både den offentlige sektor og private aktører. Disse aftaler skal derefter udmøntes i implementeringsplaner. Afhængigt af ambitionsniveau og kompleksitet kan der være behov for at udarbejde fælles målarkitektur og migreringsstrategi. Dette er fx gældende på sundhedsområdet, som netop udarbejder et målbillede for samtykke og frabedelse i forbindelse med databehandling på sundhedsområdet.

Aftaler mellem offentlige parter kan indgås som led i den kommende fællesoffentlige digitaliseringsstrategi eller kommende økonomiaftaler, hvor ansvar for koordinering og målopfølgning ligeledes kan aftales. Desuden kan der indgås aftaler med relevante private aktører eventuelt via interesseorganisationer.

3. Jura

Formålet med dette afsnit er at give en overordnet introduktion til lovgivning om og regler for behandling af personoplysninger samt give eksempler på andre former for samtykke end det, som følger af de generelle databeskyttelsesregler.

Generel lovgivning

Databeskyttelsesforordningen (GDPR) fastlægger de generelle regler for databeskyttelse og gælder for behandling af oplysninger om personer, dvs. fysiske personer, som foretages af offentlige myndigheder og af private virksomheder, foreninger, mv. Forordningen

fastlægger bl.a. betingelser for behandling af personoplysninger. Samtykke er en blandt flere mulige hjemler til behandling af personoplysninger, og der er en række krav, når samtykke anvendes som behandlingshjemmel.

Databeskyttelsesloven fastsætter supplerende nationale bestemmelser om behandling af personoplysninger inden for det nationale råderum, som databeskyttelsesforordningen giver mulighed for.

Der er desuden danske regler om behandling af personoplysninger i en række love. Lovgivning kan også stille krav om indhentelse af samtykke til fx igangsættelse af en indsats eller en undersøgelse. Af eksempler på lovgivning, som handler om behandling af personoplysninger og forskellige former for samtykke, kan desuden nævnes:

- Forvaltningsloven
- Lov om retshåndhævende myndigheders behandling af personoplysninger (Retshåndhævelsesloven)
- Lov om retssikkerhed og administration på det sociale område (Retsikkerhedsloven)
- Lov om social service (Serviceloven).

Muligt behov for ændring af lovgivning

Det kan ikke udelukkes, at anvendelse af en fællesoffentlig løsning for digitalt samtykke og frabedelse forudsætter ændring af sektorlovgivning såvel som etablering af generel hjemmel til at registrere, opbevare og dele samtykker og frabedelser i en fælles lagerkomponent. Sidstnævnte skal afklares af Digitaliseringsstyrelsen, mens eventulle behov for ændring af sektorlovgivning i alle tilfælde skal afklares i de relevante domæner.

Samtykke og frabedelse på sundhedsområdet

På sundhedsområdet i Danmark er begreberne samtykke og frabedelse indskrevet i sundhedsloven. Generelt gælder det, at sundhedspersoner kan få indsigt i helbredsinformationer uden borgerens samtykke, under forudsætning af at borgeren er i aktuel behandling hos sundhedspersonen, og at der indhentes information, der er relevant for den aktuelle behandling. Bortset fra visse undtagelser[1] vil borgeren i alle øvrige tilfælde skulle give sit samtykke til indhentning og videregivelse af helbredsinformationer.

Derudover kan en borger frabede sig indsigt i udvalgte dele af sine helbredsinformationer. Endeligt kan visse autoriserede sundhedspersoner foretage værdispringshandlinger, som sætter borgerens ønsker om beskyttelse ud af spillet, hvis "indhentningen er nødvendig til berettiget varetagelse af en åbenbar almen interesse eller af væsentlige hensyn til patienten, herunder en patient, der ikke kan varetage sine interesser, sundhedspersonen eller andre patienter", som det står i sundhedsloven.

Sundhedsområdets samtykkebegreb er således opbygget så der søges en balance mellem borgerens ret til privatlivsbeskyttelse og borgerens ret til effektiv og god behandling, hvor adgangen til vigtige helbredsinformationer kan være afgørende for kvaliteten af behandlingen.

[1] Generelt er sundhedsloven indrettet således, at når sundhedsfaglige får ret til at indhente eller videregive borgerens oplysninger uden samtykke, får borgeren samtidig en ret til at frabede sig dette.

Behovet for informeret samtykke fra en forsøgsperson til at deltage i et forskningsprojekt er reguleret i komiteloven (lov om videnskabsetisk behandling af sundhedsvidenskabelige forskningsprojekter).

4. Sikkerhed

Sikkerhedsmodel

Et samtykke eller en frabedelse kan indeholde følsomme personoplysninger – endda kan selve eksistensen af et bestemt samtykke eller frabedelse være følsomt. I en kommende infrastruktur, hvor samtykker og frabedelser kan anvendes på tværs af aktører, er der derfor behov for styring af synlighed og adgange til samtykker. De infrastrukturkomponenter, som implementerer fælles lagre, skal på deres API (fx 'hent samtykke' eller 'fremsøg samtykke') kunne håndhæve relevante adgangspolitikker. Derfor vil opmærkning af samtykker og frabedelser være relevant i datamodellen.

Her beskrives alene de vigtige principper i forhold til den overordnede, generelle sikkerhedsmodel:

1. Fagsystemet skal opmærke samtykker og frabedelser med rettigheder, inden de gemmes i lageret
2. Autorisation af fagsystemer sker på organisations eller domæneniveau, da dette vil variere mellem domæner og implementeringer.
3. Der sker to lag af filtreringer / adgangskontrol:
   i) Infrastrukturen kender kun infrastrukturens brugere.
   ii) Fagsystemets brugere er (alene) fagdomænets anliggende.

Ansvar

Ansvaret for den konkrete anvendelse, herunder lokal brugerstyring, påhviler den organisation, der anvender den enkelte samtykke og frabedelse.

Den tværgående infrastrukturs opgave er at understøtte håndhævelsen af dette ansvar lokalt og i domæner, men den kan ikke i sig selv sikre håndhævelsen lokalt og i domæner på enkeltbrugerniveau.

Ud over den egentlige forretningsanvendelse af den fælles infrastruktur kan der være behov for at give særlige tekniske medarbejdere en bred adgang til et delt lager med samtykker og frabedelser. Det kan fx være i forbindelse med support, hvor det er en forudsætning for at kunne fejlsøge eller yde bistand til brugerne. Ansvaret for tekniske medarbejderes adgang påhviler den supportgivende organisation og skal underlægges fortrolighedsaftaler.