Indholdsfortegnelse

Figuroversigt

Ledelsesresume

I denne rapport beskrives rammerne for et system, der kan sikre, at samtykker kan indhentes, dokumenteres og stilles digitalt til rådighed for SEGES fagsystemer og databaser. Systemet vil i den beskrevne form både kunne håndtere de tværgående 'big-data' samtykker og samtykker til markedsføring, som er beskrevet i Bech-Bruun rapporten, samt de samtykker, der allerede i dag indhentes til Ø90 og Kvægdatabasen. Systemet understøtter, at en del af samtykkerne skal indhentes gennem DLBR virksomhederne.

En væsentlig udfordring ved etablering af et tværgående samtykkesystem består i identifikationen af firmaet og personerne, som et samtykke skal indhentes fra. I rapporten er forudsat, at firmaet altid kan identificeres via et CVR nummer, og at ejerne, der skal indhentes samtykke fra, kan identificeres via ét eller flere CPR numre, og at denne CVR-CPR relation kan leveres af fagsystemerne, eller kan hentes via et register udenfor samtykkesystemet. Det er tilsvarende forudsat, at kontaktinformationerne til fremsendelse af samtykket kan hentes herfra. Vi har i undersøgelsen fået indikationer fra fagsystemerne på at dette er muligt, men undersøgelsen har ikke været udtømmende, og bør forfølges yderligere.

En anden væsentlig forudsætning er at samtykkesystemet ikke tillægger samtykkerne nogen betydning, men alene stiller dem til rådighed for fagsystemerne på anfordring. Det er fagsystemet, der skal vide hvilket samtykke der skal spørges på, for at en given handling har tilstrækkelig retshjemmel – f.eks. en tværgående dataanalyse.

Rapporten er at betragte som en foranalyse, og vil kræve et yderligere og tættere analysearbejde med fagsystemerne og juridiske rådgivere.

Formål

Formålet med dette delprojekt er at vurdere, hvorledes SEGES kan sikre og dokumentere de samtykker, der er beskrevet i rapporten "Anvendelse af personoplysninger i SEGES' databaser" fra Advokatfirmaet "Bech-Bruun" (Marts 2015).

Analysen vil tage udgangspunkt i de delsystemer, der henvises til i Bech-Bruun rapporten: Ø90, Dansk Markdatabase samt Kvægdatabasen, samt de to identificerede samtykker (efterfølgende "de to generelle samtykker"):

1. Samtykke til selvstændig analyse og samstilling af personlige data
2. Samtykke til at rette henvendelse til den enkelte landmand

Målet er at analysere og beskrive en teknisk løsning for hvorledes disse samtykker kan indhentes, dokumenteres og stilles til rådighed for systemerne/databaserne.

Endvidere vil mulighederne for at generalisere den tekniske løsning til også at kunne håndtere fremtidige samtykker og andre systemsammenhænge end de, der er beskrevet i Bech-Bruun rapporten, blive vurderet.

Rapporten udgør den tekniske del af vurderingen af, hvorledes samtykker kan indhentes og dokumenteres, der leveres som en del af outputtet under delopgaven "Privacy" i forbindelse med "Arbejdspakke 1: Integration og dataanalyse i en Big Data kontekst" under projektet "Maksimal dataudnyttelse på landbrugsbedriften" 2015.

Den gennemførte undersøgelse

Rapporten er baseret på interviews og samtaler med repræsentanter fra fagsystemerne Ø90/Økonomidatabasen (Torben Vestergaard), Dansk Markdatabase (Jens Bligaard) og Kvægdatabasen (Vibeke Christensen), samt Dorthe Laursen (Jura) og Peter Enevoldsen (IT).

I det følgende er givet et resume af de informationer og krav vedrørende samtykker, der kom frem under de gennemførte samtaler, og implikationerne af disse for et fremtidigt samtykkesystem er beskrevet.

Krav fra fagsystemerne

Udover de to generelle samtykker i formålsbeskrivelsen som vil skulle indhentes, så de dækker alle tre fagsystemer, er der for økonomi- og kvægområdet identificeret yderligere samtykker, som indhentes i dag, og som med fordel vil kunne indarbejdes i et fremtidigt samtykkesystem.

Ø90/Økonomidatabasen

Landmandens økonomidata registreres i Ø90 og data overføres herfra til Økonomidatabasen, hvorfra der laves forskellige analyser på landmandens data. Til dette indhentes et samtykke fra landmanden i tre niveauer:

1. Samtykke til at bruge data til statistiske formål
2. Samtykke til anonymiseret benchmarking
3. Samtykke til ikke-anonymt "business check"

Da dataansvaret ligger hos DLBR virksomhederne er det dem, der skal indhente samtykkerne. Dette sker ved at DLBR virksomheden eller SEGES printer en samtykkeformular, og DLBR virksomheden sørger efterfølgende for at indhente landmandens underskrift. Dette sker typisk på et personligt møde, hvor DLBR virksomheden motiverer samtykket overfor landmanden. En kopi af formularen sendes efterfølgende til SEGES, hvor en sekretær i SEGES Økonomi & Virksomhedsledelse indberetter samtykket i Ø90/Økonomidatabasen.

Timingen af hvornår der skal indhentes et samtykke, samt identifikationen af hvilken eller hvilke personer, de skal indhentes fra, håndteres i Ø90, hvor bedrifternes organisering og ejerforhold er modelleret. Ø90 ved eksempelvis, om en bedrift har flere ejere og der derfor skal indhentes flere personlige samtykker. Via Ø90 afgør DLBR virksomhederne og SEGES endvidere, om der skal indhentes nye samtykker ved ændringer i ejerforhold - eksempelvis ejerskifte.

Markedet for landbrugsrådgivning er meget konkurrencepræget, og det sker derfor at landmændene skifter center, eller køber deres rådgivning fra forskellige centre. Når en landmand skifter center, er det normalt at papirsamtykkerne enten flyttes med, eller det nye center indhenter nye samtykker. Informationerne om hvilket center der giver landmanden økonomirådgivning findes i Ø90.

Implikationer for samtykkesystemet

Hvis Ø90 samtykkerne skal indarbejdes i et fremtidigt samtykkesystem, er det værd at hæfte sig ved følgende:

- Initiativ ligger i Ø90
  Forretningslogikken omkring hvornår samtykker skal indhentes eller udløber – eksempelvis på grund af ejerskifte eller centerflytning - kan håndteres af Ø90.

- Personen eller firmaet identificeres af Ø90
  Kortlægningen af hvilke firmaer og personer, der skal indhentes samtykker fra, sker allerede i Ø90.

- Formidleren af samtykket ligger i Ø90
  Ø90 ved hvilken DLBR virksomhed, der skal indhente samtykket.

Dette betyder, at såfremt samtykkesystemet skal stå for selve indhentelsen af samtykket, kan instruksen om hvem, det skal indhentes fra, hvornår og via hvilken DLBR virksomhed, komme fra Ø90 – det er ikke nødvendigt at kortlægge dette i selve samtykkesystemet.

Hvis samtykkesystemet skal stå for at indhente samtykkerne, er det endvidere klart, at der skal udvikles funktionalitet, der understøtter at dette sker via DLBR virksomhederne. Dette er uanset om systemet alene skal håndtere de to generelle samtykker eller også skal omfatte de Ø90 specifikke samtykker, der indhentes i dag. Dette skyldes at Økonomi & Virksomhedsledelse vurderer, at såfremt de generelle samtykker også skal omfatte økonomidata, *skal* de indhentes gennem den dataansvarlige DLBR virksomhed – også selvom SEGES på Mark og Kvægområdet selv står som dataansvarlig.

Digitalisering og effektivisering af den manuelle samtykkeproces med DLBR virksomhederne bør desuden overvejes som en forretningsmulighed.

Kvægdatabasen

SEGES er dataansvarlig for Kvægdatabasen og kan (og skal) derfor selv indhente de fornødne samtykker hos landmanden. I dag indhentes samtykke fra landmanden på om et givet firma – eksempelvis en dyrlægepraksis – må trække informationer om landmandens kvægbedrift fra DMS. Dette sker typiske ved at landmanden eller dyrlægen fra DMS printer en formular, som landmanden underskriver og sender til SEGES, der registrerer samtykket i DMS.

Timingen af samtykket udløses af Landmanden eller dyrlægen via DMS, der identificerer hvilket CVR eller CPR nummer, der er brug for samtykke fra. I samtykketeksten er angivet hvilket firma eller navngiven person samtykket gælder for (eksempelvis dyrlægepraksis eller navngiven dyrlæge). Disse informationer findes i DMS.

Implikationer for samtykkesystemet

Hvis de eksisterende DMS samtykker skal implementeres i samtykkesystemet:

- Initiativ ligger i DMS
  Ligesom for Ø90 initieres det at der skal indhentes et samtykke fra DMS/Kvægdatabasen.

- Personen eller firmaet identificeres af Kvægdatabasen
  DMS identificerer personen eller firmaet, der skal indhentes samtykke fra via et CPR eller CVR nummer.

- Parameterstyrede samtykker
  Da samtykket eventuelt omfatter en eller flere kvægbedrifter og giver rettigheder til et bestemt firma eller en person, vil dette sandsynligvis kræve, at samtykkerne i samtykkesystemet kan parameterstyres fra fagsystemet. Eksempelvis at DMS kan indskyde navn og adresse på en dyrlægepraksis i samtykket.

Dansk Markdatabase

SEGES er dataansvarlig og indhenter i dag ikke samtykker fra landmanden. Aktien i et fremtidigt samtykkesystem vil være håndteringen af de to generelle samtykker.

Juridiske krav til samtykkesystemet

Baseret på det juridiske input i undersøgelsen, er der stillet følgende krav til samtykkesystemet:

Samtykket skal være personligt

Data i SEGES systemer er oftest persondata, og samtykket skal derfor være afgivet af de implicerede personer. Dette betyder eksempelvis at elektronisk NemID signering af et samtykke, skal være baseret på den personlige og CPR henførbare NemID og ikke den mere brede NemID Erhverv. Det betyder samtidig, at et CVR nummer på en landbrugsbedrift, der er ejet af flere personer, kræver et samtykke fra hver enkel af personerne, før samtykket for CVR enheden er tilstrækkeligt.

Styrke i bevisførelsen vs. brugervenlighed

Det skal via samtykkesystemet kunne bevises hvem der har givet samtykke, til hvad (den præcise samtykketekst) samt hvornår. Den stærkeste bevisførelse ligger her i enten et personligt NemID signeret dokument eller et papirsamtykke underskrevet med vitterlighedsvidner.

Ovennævnte er forholdsvist omstændelige og kan udfordre brugervenligheden. I situationer hvor konsekvenserne ved at tabe en samtykketvist ikke er så voldsomme, er der ønske om at lade brugernes elektroniske underskrift erstatte af hurtigere og mere brugervenlige godkendelser, hvor bevisførelsen er svagere, men dog stadig til stede.

Samtykkesystemet skal derfor understøtte følgende former for samtykke accept:

- **NemID Signering (stærk)**
  Samtykkedokumentet er signeret med brugerens personlige NemID, og kan derfor entydigt henføres til et CPR nummer og en eksakt samtykketekst. Brugervenligheden er begrænset men bevisførelsen er stærk.

  Velegnet til: Personoplysninger, "Samtykke til selvstændig analyse og samstilling af personlige data" samt eventuelt fremtidige versioner af Ø90 samtykkerne og DMS samtykkerne.

- **Papirunderskrift (stærk)**
  Samtykkedokumentet er underskrevet af landmanden og scannes ind i samtykkesystemet af en indlogget DLBR eller SEGES konsulent. Brugervenligheden er lav, men bevisførelsen er stærk (kopi af det underskrevne samtykke kan altid genfindes).

  Velegnet til: Personoplysninger, "Samtykke til selvstændig analyse og samstilling af personlige data" samt den eksisterende version af Ø90 samtykkerne og DMS samtykkerne.

- **SEGES Fælles Login (svag)**
  Landmanden er logget ind med DLBR Fælles Login og præsenteres for en samtykketekst, som landmanden godkender ved eksempelvis at trykke på en knap eller sætte et flueben. Brugervenligheden er høj, men bevisførelsen er svagere. Der er ikke tale om signering, men blot en registrering i en database af, at brugeren har været logget ind og accepteret samtykket. SEGES kundecenter og SEGES udvikling/drift har adgang til at sætte brugernes kodeord og rette i databaser, hvilket vil kunne anføres af modparten i en tvist. Dog er brugerens login og accept skrevet i loggen.

  Velegnet til: "Samtykke til at rette henvendelse til den enkelte landmand", Nyhedsbreve, Vilkår ved brug af websites.

De generelle samtykker skal indhentes via DLBR

I forhold til de to generelle samtykker - "Samtykke til ikke-anonym databehandling" og "Samtykke til markedsføring" – er udfordringen som nævnt, at såfremt de også skal omfatte økonomidata, vil de sandsynligvis skulle indhentes via DLBR virksomhederne. Dette upåagtet at SEGES på Dansk Markdatabase og Kvægdatabasen selv er dataansvarlig, og her kunne indhente dem udenom DLBR. Samtykkesystemet kan supplere med et modul, der understøtter indhentning af samtykker gennem DLBR. Da de fleste

DLBR konsulenter og centre er kendt af DLI Brugerdatabasen, har vi allerede infrastukturen til at udvikle dette.

Historik

Det er et krav at samtykkesystemet indeholder en historik på den enkelte persons samtykke – hvornår og hvordan er det accepteret, af hvem og hvad var den eksakte samtykketekst, samt efterfølgende hændelser – eksempelvis tilbagekaldelse af samtykket. Efterfølgende ændringer i samtykketeksten skal selvsagt ikke slå igennem på allerede underskrevne samtykker.

Samtidig skal samtykkesystemet indeholde en komplet historik på ændringer i selve samtykket – eksempelvis ændringer i tekst og vilkår, samt hvilke bruger der har udført disse.

Funktionelle krav til samtykkesystemet

Vi har i arbejdet med at afdække de funktionelle krav til systemet, anvendt en ”brugsscenarie” orienteret proces. Vi startede med at identificere de forskellige aktører (roller) der forventes at anvende systemet. Med udgangspunkt i de identificerede roller har vi efterfølgende udledt de funktionelle krav, som de enkelte roller stiller til samtykkesystemet. I det følgende defineres først rollerne, hvorefter de funktionelle krav gennemgås.

Roller

- Landmanden
  Denne rolle dækker over de personer, der afgiver det faktiske samtykke til, at den dataansvarlige må anvende deres personlige data i henhold til samtykketeksten.

- Fagsystemer
  Denne rolle dækker automatiske processer der forespørger samtykkesystemet for at sikre, at det nødvendige samtykke er afgivet i forhold til at udføre en operation på personlige data (eksempelvis Ø90).

- SEGES konsulenten
  Denne rolle dækker ansatte ved SEGES P/S der forespørger samtykkesystemet som dataansvarlig eller databehandler. Systemet er kun tiltænkt at understøtte samtykker vedr. databaser hvor SEGES P/S fungerer som enten dataansvarlig eller databehandler. Som følge deraf må alle der anvender samtykkesystemet som rollen ”SEGES konsulent” se alle data, og der er derfor ikke beskrevet en segmenteret adgang til data for denne rolle.

- DLBR konsulenten
  Ansatte ved de enkelte centre der anvender samtykkesystemet i kraft af deres ansættelse ved dataansvarlig.

- SEGES jurist
  Person med den fornødne juridiske viden til at definere en samtykke tekst samt krav til afgivelse af samtykke.

- Supporter
  Ansat ved SEGES P/S der varetager intern- og ekstern slutbruger support af SEGES P/S systemer.

- Driftsansvarlig
  Ansat ved SEGES P/S der varetager drift og overvågning af SEGES P/S systemer.

Funktioner

Landmanden

Afgive samtykke

Når et konkret samtykke er ønsket afgivet skal den person samtykket er ønsket af, være i stand til at afgive samtykke. Vi har identificeret 3 måder hvorved et samtykke kan afgives:

- Online uden signering
  Når samtykkes afgives online uden signering, besøger personen der afgiver samtykke en webside, der ligger bag login (brugernavn/password). Efter login kan samtykketeksten gennemlæses og efterfølgende accepteres. Det er således udelukkende kombinationen af brugernavn og password der verificerer, at personen der afgiver samtykke er den "rigtige". Denne metode til afgivelse af samtykke, påtænkes anvendt til "mindre tunge" samtykker, som f.eks. samtykke til at modtage mails med henvendelser fra SEGES P/S eller samarbejdspartnere.

- Online med signering
  Når samtykke afgives online med signering, besøger personen der afgiver samtykke en webside. hvor samtykketeksten kan gennemlæses. Ved afgivelse af samtykke signeres teksten med personens personlige NemID. Såfremt personens CPR nummer er kendt, er det vha. NemID muligt at få personen til at bekræfte sit CPR nummer ved indtastning og derved verificere. at signatur og CPR nummer stemmer overens. Det er således NemID der verificerer, at personen der afgiver samtykke er den "rigtige".

- Underskrift på papir
  Når samtykke afgives ved underskrift på papir, udprintes samtykketeksten fra samtykkesystemet, og personen afgiver samtykke ved fysisk at underskrive teksten. Det fysiske dokument skal derefter opbevares og det er det fysiske dokument, der verificerer at personen der afgiver samtykke er den "rigtige".

Den ovenstående liste over "verificeringsmetoder" skal ikke ses som udtømmende, men beskriver de metoder vi igennem vores analyse har identificeret som ønskede. Samtykkesystemet kan sagtens forestilles at blive udvidet med yderligere verificeringsmetoder over tid.

Afvise samtykke

I alle scenarier hvor en person får mulighed for at afgive et samtykke, der registreres af samtykkesystemet, skal det være muligt at afvise det ønskede samtykke. Denne afvisning skal ligeledes registreres af systemet. Registreringen af at et samtykke er afvist kan f.eks. anvendes til ikke at udsende påmindelser om ønsket samtykke til personer, der allerede har afvist det.

Se afgivne samtykker

De personer der har afgivet samtykke, skal i en selvbetjeningsløsning kunne de disse afgivne samtykker. Det skal således være muligt at tilgå en webside, hvor personen kan identificere sig og efterfølgende se sine afgivne samtykker.

Tilbagekalde samtykke

I selvbetjeningsløsningen skal det være muligt at tilbagekalde (annullere) afgivne samtykker.

Fagsystemer

Anmode om afgivelse af samtykke
Når et forretningssystem har brug for et samtykke for at gennemføre en automatisk proces, skal systemet kunne registrere dette behov hos samtykkesystemet, således at indhentning af samtykket kan påbegyndes.

Data i fagsystemerne er registreret med anvendelse af CVR nummer som nøgle. En anmodning om samtykke vil derfor være en anmodning om, at den eller de personer, hvortil dataene kan regnes som personfølsomme (ejeren eller ejerne af CVR nummeret), skal afgive samtykke. Vi forventer, at de relevante Fagsystemer selv kender denne relation, og at det derfor er indeholdt i forespørgslen. En anmodning om samtykke bliver således et CVR nummer i kombination med en eller flere personidenter, der identificerer de personer hvorfra samtykke skal indhentes.

I nogle tilfælde ønskes samtykket indhentet vha. et DLBR center og ikke direkte fra den ønskede person. I dette tilfælde forventes forespørgslen om anmodning også at indeholde en identifikation af hvilket center der skal indhente samtykket.

Forespørge om afgivet samtykke
Relationen imellem CVR nummer og person identer, der er indeholdt i en anmodning om samtykke registreres i samtykkesystemet, når anmodningen modtages. Fagsystemerne kan herefter anvende CVR nummeret som nøgle, når de forespørger samtykkesystemet om hvorvidt samtykket er afgivet. Hvis – og kun hvis – der findes samtykke fra alle de person identer, der var indeholdt i anmodningen, svarer samtykkesystemet tilbage, at der er afgivet samtykke.

SEGES konsulenten

Anmode om afgivelse af samtykke
SEGES konsulenter der i kraft af deres ansættelse har behov for at igangsætte processen med indhentelse af samtykke, kan igennem samtykkesystemets brugergrænseflade gøre dette. Som med fagsystemer der gør det som en del af en automatiseret proces, kræver den manuelle igangsættelse at konsulenten angiver CVR nummeret for den virksomhed hvis data afkræver samtykket. Samtidigt skal der angives person identer for de personer samtykket skal indhentes fra.

Det er igen vigtigt at understrege, at relationen imellem virksomheden angivet ved CVR nummer og de personidenter fra hvem der skal indhentes samtykke, alene er konsulentens ansvar. Samtykkesystemet holder denne relation med henblik på forespørgsel vha. CVR nummer, men laver ingen validering af, at de angivne personer er inkluderet eller udtømmende for CVR nummeret.

Forespørge om og se afgivet samtykke
Igennem samtykkesystemets brugergrænseflade kan ansatte ved SEGES P/S, der som en del af deres arbejdsopgave har behov for dette, fremsøge afgivne samtykker i systemet. Samtykker kan fremsøges ved CVR nummer, hvorved status for de enkelte personlige samtykker herunder kan ses. Endvidere kan samtykker fremsøges vha. personidenter, hvorved afgivne samtykker fra den specificerede person kan ses. For et enkelt personligt samtykke er det muligt at se hvilken oprindelig samtykkeanmodning (CVR nummer) samtykket er en del af. Det er muligt at se samtykketeksten, samt hvornår samtykket er afgivet eller afslået. Såfremt samtykket efterfølgende er tilbagetrukket, vil dette også fremgå af visningen.

SEGES juristen

Oprette ny samtykkeskabelon
Når en jurist har identificeret og skrevet en ny samtykketekst, skal denne kunne oprettes i samtykkesystemet. Juristen - eller en person der handler på juristens vegne - kan igennem samtykkesystemets bru-

gergrænseflade gøre dette. Sammen med teksten forventer vi, at der skal angives diverse metadata om samtykkeskabelonen, som f.eks. tilladte verificeringsmetoder (SEGES fælles login, NemID og/eller fysisk underskrift) og tilladte leveranceteknikker (fysisk brev, e-mail, via DLBR konsulenter, etc.).

Vi har i forbindelse med interviews med kvæg vurderet muligheden for at parametisere samtykketeksterne. Dette skal forstås således, at enkelte ord eller sætninger i samtykketeksten ved oprettelse, kan erstattes af navngivne "placeholders". Når et forretningssystem efterfølgende anmoder om et samtykke af den type, så skal der medsendes en parameterliste med de fornødne værdier, der skal erstatte de indsatte placeholders. Teknisk vil en sådan løsning være overkommelig at løfte. Det tilfører dog anvendelsen af systemet en betydelig kompleksitet, og det vil være nødvendigt at analysere de juridiske implikationer.

Redigere samtykkeskabelon

Rettelser der udelukkende har kosmetisk karakter (stavefejl, kommatering etc.) vil umiddelbart kunne gennemføres, såfremt det skønnes formålstjenstligt, at systemet skal understøtte en sådan funktion. Rettelser i teksten med juridiske implikationer (f.eks. for smalt et samtykke) er mere komplekse, og vi har i vores analyse identificeret 3 muligheder for at supportere sådanne.

Option A: Der kan kun foretages "kosmetiske" rettelser i eksisterende samtykkeskabeloner. Rettelser af juridisk karakter kræver at en ny samtykkeskabelon oprettes. Fagsystemer der anvender den gamle samtykkeskabelon omkodes således at de forespørger på den nye samtykkeskabelon. Alle personer der har afgivet samtykke til den gamle skabelon skal på ny afgive samtykke til den nye skabelon. Alle nye personer skal udelukkende give samtykke til den nye skabelon.

Option B: Der kan kun foretages "kosmetiske" rettelser i eksisterende samtykkeskabeloner. Rettelser af juridisk karakter kræver at en ny samtykkeskabelon oprettes. Eksisterende Fagsystemer forespørger fremadrettet på den gamle skabelon. Nye Fagsystemer der kræver den nye skabelon forespørger på denne. Alle personer der har afgivet samtykke til den gamle skabelon skal udelukkende give samtykke til den nye skabelon. Alle nye personer skal give samtykke til såvel den gamle som den nye skabelon.

Option C: Der kan foretages "kosmetiske" rettelser *og* rettelser af juridisk karakter i eksisterende samtykkeskabeloner. Rettelser af juridisk karakter skal omfatte den gamle tekst, således at den nye tekst som minimum inkluderer det gamle samtykke. Eksisterende Fagsystemer forespørger uændret på den gamle version af teksten, der fortsat er dækkende for deres behov. Nye Fagsystemer forespørger på den nye version af teksten. Alle personer der har givet samtykke til den gamle tekst, behøves kun at give samtykke til den nye tekst såfremt de skal anvendes i/af de nye Fagsystemer. Nye personer giver udelukkende samtykke til den nye tekst, da denne omfatter den gamle tekst.

Lukke samtykkeskabelon

Hvis en jurist identificerer et samtykke, der ikke længere skal anvendes, skal det være muligt igennem samtykkesystemets brugergrænseflade, at markere dette som lukket. De samtykker der evt. allerede er afgivet på den samtykkeskabelon, der ønskes lukket, skal naturligvis forblive i systemet. Det er derfor ikke muligt at slette en samtykkeskabelon, men ved at markere den som lukket, kan der ikke foretages nye anmodninger om samtykke baseret på denne skabelon.

Supporter

Vi forudsætter at support vedr. samtykker håndteres af de specifikke fagsystemer, der definerer samtykket. Således er supportrollen ikke tænkt ind i samtykkesystemet, og har derfor ikke afledt funktionelle krav.

Driftsansvarlig

Vi har ikke identificeret krav eller opgaver, der ligger ud over hvad der normalt kan forventes for at drifte en lignende løsning, og rollen har derfor ikke afledt specifikke funktionelle krav.

Sikkerhed og rettigheder

Da alle samtykker i samtykkesystemet forventes at være relevante for SEGES P/S enten i rollen af dataansvarlig eller databehandler, er der ingen segmenteret adgang til data for SEGES P/S medarbejdere eller SEGES P/S Fagsystemer. Det eneste scenarie der skal behandles individuelt, er skrivning (oprettelse/redigering) af samtykke typer. Derudover skal DLBR konsulenter udelukkende kunne se de afgivne samtykker, de selv har indhentet.

Løsningen tænkes sikret af SEGES fælles login, hvor SEGES P/S medarbejdere og DLBR konsulenter allerede har eksisterende logins. De nødvendige rettighedsgrupper oprettes i SEGES fælles login og udleveres som claims ved login. De nødvendige sikkerhedsgrupper er:

- SEGES samtykke forretningssystem
  Fagsystemer der i automatiske processer anvender samtykkesystemet, skal være i denne gruppe. Gruppen giver således adgang til at anmode om afgivelse af samtykker eller at forespørge om hvorvidt samtykker er afgivet. Der påtænkes ingen yderligere segmentering og alle fagsystemer i gruppen kan derfor anmode og forespørge om alle typer af samtykker, uden begrænsninger i CVR numre eller person identer.

- SEGES P/S samtykke bruger
  Personer ansat ved SEGES P/S der i kraft af deres arbejde har brug for læse adgang til data i samtykke systemet, tildeles denne gruppe. Gruppen giver således adgang til at se afgivne samtykker samt anmode om samtykker igennem samtykkesystemets brugergrænseflade. Der påtænkes ingen yderligere segmentering og alle ansatte i gruppen kan derfor se alle afgivne samtykker, samt anmode om samtykker uden begrænsning i CVR numre eller person identer.

- SEGES P/S samtykke administrator
  Personer ansat ved SEGES P/S til at formulere samtykker tildeles denne gruppe. Gruppen giver således adgang til at oprette nye samtykketyper samt redigere eksisterende samtykketyper. Der påtænkes ingen yderligere segmentering, og personer i gruppen kan derfor oprette alle typer af samtykketyper samt redigere alle eksisterende samtykketyper.

Definition af samtykkebegreber

Samtykkeskabelon

En tekst der beskriver et samtykke. Teksten kan variere (via erstatning af placeholders) på data, der er tilgængelige i samtykkesystemet, eksempelvis samtykkenøgle og persondatainteressentid. Kan ikke variere på fagsystemsspecifikke data, fx regnskabsnummer.

Samtykke

Kombinationen af samtykkeskabelonen med data.

Afgivet samtykke

Registrering af at en persondatainteressent har afgivet samtykke til et specifikt samtykke.

Samtykkenøgle
En streng der grupperer et sæt på en eller flere persondatainteressenter, der alle skal afgive samtykke, før der er givet samtykke til hele samtykkenøglen. Typisk enten et CVR-nummer for virksomheder eller et CPR-nummer eller en e-mailadresse for personer.

Samtykkeindhentning
Processen med at registrere samtykker fra en mængde af persondatainteressenter for en given samtykkenøgle. Denne rapport behandler ikke detaljeret hvorledes samtykkeindhentning skal foregå men forudsætter, at der eksisterer en proces (eventuelt manuel) omkring dette.

Persondatainteressent
En person der kan give samtykke til en samtykkeskabelon. Identificeret ved et CPR-nummer eller en e-mailadresse.

Afgrænsning
I dette afsnit beskrives forskellige afgrænsninger og forudsætninger, der er gjort omkring samtykkesystemet.

Indhentning af samtykker
Samtykkesystemet kan implementeres i flere tempi – indledningsvist kan implementeres en udgave, hvor der eksisterer en manuel proces for indhentning af samtykker for persondatainteressenter.

Systemet kan efterfølgende udvides til at omfatte arbejdsprocesserne omkring indhentning, men dette vil kræve en nærmere analyse, som endnu ikke er gennemført. Man kan forestille sig at samtykkesystemet automatiserer processen med udgangspunkt i:

- De til samtykkeskabelonen specificerede krav til hvem der skal indhente samtykke
  - SEGES
  - DLBR virksomhed

- De af Fagsystemerne leverede personidentifikationsdata
  - CPR
  - E-mailadresse
  - Postadresse
  - SEGES Login BrugerID

- De til samtykkeskabelonen specificerede krav til hvilken type af samtykke der er påkrævet
  - Fysisk underskrift
  - Accept af samtykke bag SEGES Login
  - NemID signering

Hvor det er muligt kan samtykkesystemet formidle forespørgslen på samtykke til de persondatainteressenter hvor de nødvendige informationer er til stede - eksempelvis en e-mailadresse leveret af forretningssystemet, fysisk brev til dem hvor der kun forefindes postadresse osv. - og sender residualet (fx hvor der kræves fysisk underskrift, men der kun forefindes en e-mailadresse) til manuel behandling. At afklare de nærmere rammer for ovenstående, er out-of-scope for denne rapport.

Identifikation af hvilke persondatainteressenter der skal indhentes samtykke fra er Fagsystemerne ansvar

Samtykkesystemet har ingen viden om sammenhængen imellem virksomhedsdata, repræsenteret ved CVR nummer, og de personer der skal afgive samtykke, for at fagsystemerne må anvende data, ud over hvad fagsystemerne har angivet i anmodningen om samtykke.

Samtykkesystemet er således ikke i stand til at svare på om de nødvendige personer har afgivet samtykke, blot om de personer fagsystemerne har anmodet om samtykke fra, har afgivet samtykke. Det er således fagsystemerne, der bliver autoritative på sammenhængen imellem samtykkenøgle (fx CVR nummer) og personer (identificeret på fx e-mailadresse, CPR-numre eller SEGES login brugerid) og den relation samtykkesystemet modellerer og gemmer, afspejler udelukkende den viden, der er formidlet fra fagsystemerne.

Ingen rettighedsmodel for hvem der må se samtykker

Alle samtykker i samtykkesystemet vedrører SEGES P/S enten i dennes rolle som dataansvarlig eller databehandler. Samtykkesystemet modellerer derfor ikke et ejerskab over de enkelte samtykker. Samtykkesystemet modellerer og gemmer hvem der indhenter et samtykke (SEGES P/S eller et specifikt DLBR center) således at samtykker kan indhentes direkte af SEGES P/S eller af et angivet DLBR center. Denne registrering går udelukkende på hvem der indhenter samtykket, men kan anvendes til at tillade DLBR centre at se de samtykker, de selv har indhentet.

En datakilde der kan skabe sammenhæng mellem CVR-numre og persondatainteressenter skal identificeres

Såfremt samtykker der anvendes af mere end et forretningssystem skal kunne understøttes, vil det være nødvendigt, at fagsystemerne er enige om hvilke personer, en given samtykkenøgle omsættes til. Det kan tale for at udskille dette ansvarsområde i et særskilt system - et Virksomheds/Persondatainteressent-registeret - men det kan også bygges som en del af de enkelte fagsystemer. For at fagsystemerne skal kunne løfte denne opgave forudsættes det, at det er muligt at finde eller opbygge en datakilde, der entydigt kan omsætte et CVR-nummer til en eller flere personer, for hvilke virksomhedens data er at opfatte som persondata. Der vil normalt være tale om ejerne, men hvilke personer der præcist drejer sig om er en juridisk vurdering. CVR-registret indeholder oplysninger om ejerandele over 5%, men det er jf. "Bekendtgørelse af lov om Det Centrale Virksomhedsregister"[1] paragraf 18 stk. 2 ikke muligt at udlede CPR-numre fra disse data som privat virksomhed.

Samtykkesystemet tillægger ikke samtykkeskabelonerne betydning - det sker i fagsystemerne

Det forudsættes at fagsystemerne har viden om sammenhænge mellem brug af data og nødvendige samtykker. Eksempelvis skal Dansk Markdatabase have viden om at en analyse, hvori der samkøres data med Kvægdatabasen, kræver samtykke X og Y for det CVR-nummer A, hvis data analysen ønskes udført på.

Ligeledes er det fagsystemernes ansvar at identificere samtykkenøglen. Visse samtykker vil være personlige, fx samtykke om markedsføring, hvor samtykkenøglen er et CPR-nummer eller en e-mailadresse. Andre vil være virksomhedsbaserede, fx samtykke om samkørsel af data på tværs af Dansk Markdatabase, Ø90 og Kvægdatabasen, hvor samtykkenøglen er et CVR-nummer. Og endeligt vil nogle samtykker være relevante både for personer og virksomheder.

Systemarkitektur

Vi forventer at implementere den beskrevne løsning i en client/server arkitektur. Serverdelen implementerer den fornødne forretningslogik, samt anvender en database til at persistere informationer vedr. samtykkeskabeloner og afgivne samtykker.

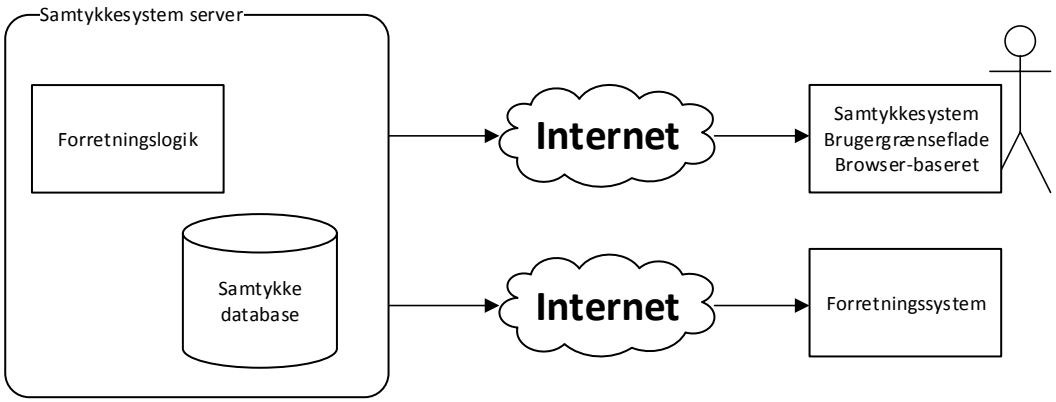
[1] https://www.retsinformation.dk/forms/r0710.aspx?id=27293

Den brugervendte klientdel forventes at være en browserbaseret løsning. Automatiserede processer der skal anvende løsningen, er ligeledes at regne som klienter i denne arkitektur, og vi forventer, at de skal kommunikere med løsningen igennem en servicesnitflade baseret på web-protokoller.

Fordelene ved en webbaseret client/server løsning er mange, men blandt de primære kan nævnes:

- Opdatering af klienterne er gnidningsfrit, idet nyeste version altid hentes til browseren fra serveren.
- Alle klienter kører altid på seneste version af forretningslogikken, da denne er centraliseret i serverdelen.
- Løsningen kan gnidningsfrit integreres med og beskyttes af "SEGES fælles login" hvis primære anvendelse er webapplikationer.

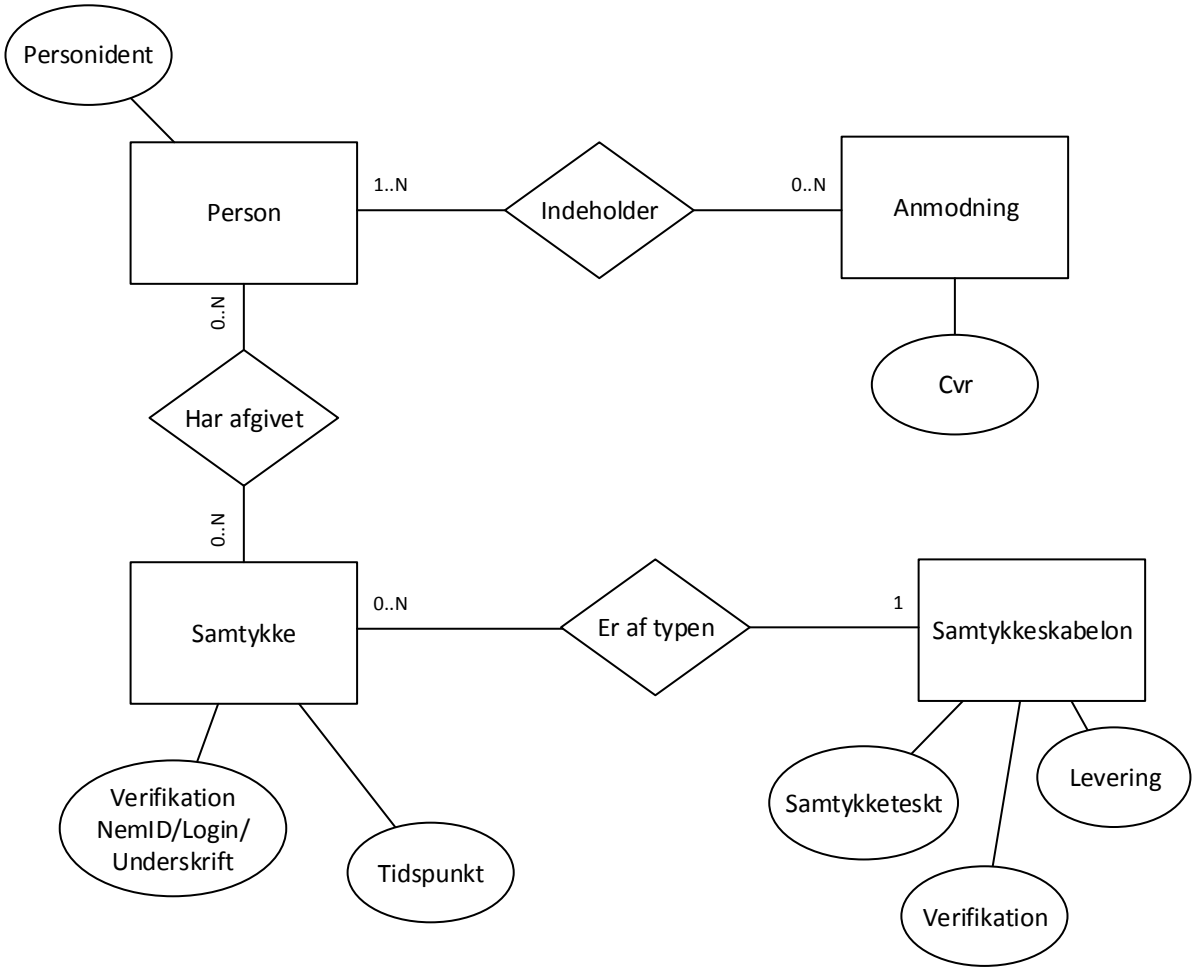
Den eneste reelle ulempe ved en webbaseret client/server løsning er, at klienterne skal have en aktiv internetforbindelse for at kunne anvende løsningen, hvilket for denne løsning næppe kan udgøre et problem.



Figur 1 Systemarkitektur

Datamodel

Nedenstående E/R diagram giver et overblik over den forventede datamodel. Det er ikke at regne som et endeligt eller udtømmende diagram, men udelukkende tiltænkt at give et overblik over nogle af de tanker, der ligger bag den forventede datamodel.

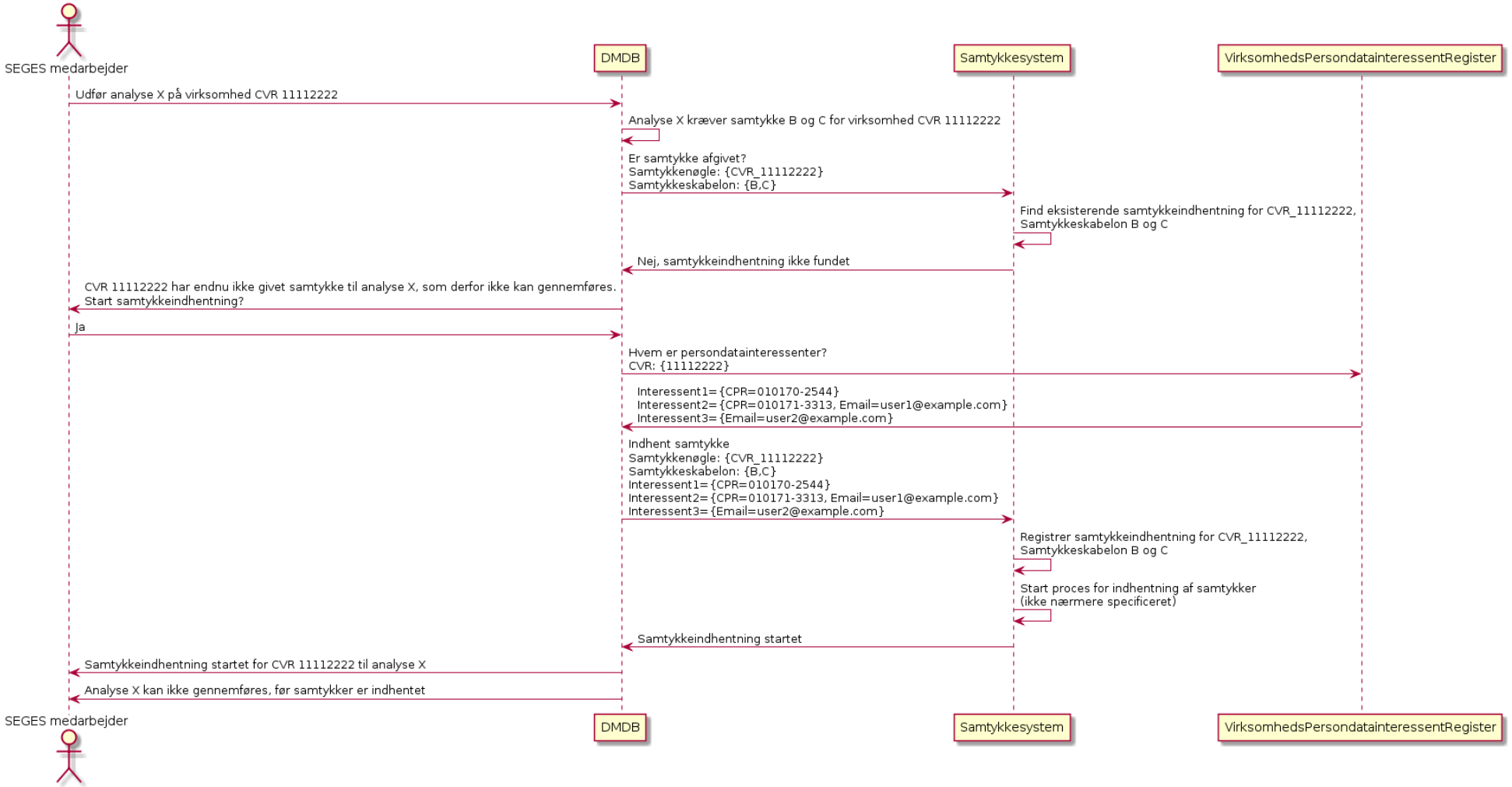


Figur 2 Datamodel

- En anmodning om samtykke er identificeret af et CVR nummer og kan ”indeholde” en eller flere personer identificeret af en ”personident” (sandsynligvis SEGES login navn eller CPR nummer). Dette modellerer at forretningssystemer anmoder om samtykke vedr. en ”klump” virksomhedsdata repræsenteret ved et CVR nummer, men at de faktiske samtykker afgives på personligt niveau.
- En person er indeholdt i nul, én eller flere anmodninger. Multipliciteten nul er her kun nødvendig, såfremt anmodninger om samtykke kan ske direkte for en specifik person og ikke kun som en del af en anmodning repræsenteret ved et CVR nummer. Multipliciteten ”mange” modellerer at vi ser personerne som unikke baseret på deres personident og at hver personident således kun optræder en gang.
- En person har afgivet nul, ét eller flere samtykker. Samtykket indeholder en verifikation af personen ved afgivelse af samtykke. Dette kan være SAML token ved SEGES fælles login, det signerede dokument ved NemID signering eller en skannet kopi ved underskrift på papir. Dette modellerer, at alle afgivne samtykker er personlige og verificerede. Ligeledes er som minimum tidspunktet for afgivelsen registreret. Multipliciteten nul er nødvendig, da samtykker kan afslås og personer anmodet om samtykker, kan således godt have nul afgivne samtykker.
- Et samtykke er af specifikt én type samtykkeskabelon. Da samtykkeskabelonen angiver samtykketeksten, samt evt. specificerer verificeringsmetode og leveringsmetode, er det naturligvis nødvendigt for et samtykke at være af én og kun en type samtykkeskabelon.

Sekvensdiagrammer

Dette afsnit indeholder en række sekvensdiagrammer, der er medtaget for at dokumentere udvalgte integrationsscenarier med samtykkesystemet.



Figur 3 Eksempel på tværgående dataanalyse

Sekvensdiagrammet i **Error! Reference source not found.** illustrerer en SEGES medarbejder, der ønsker at foretage en analyse på en virksomheds data i Dansk Markdatabase, hvor der indgår data fra andre fagområder. Netop denne analyse kræver samtykkerne B og C, hvilket er blevet defineret i DMDB da analysen blev specificeret og udviklet. DMDB ved derfor, at den inden den udfører analyse X skal sikre, at der er afgivet samtykke B og C for virksomheden med CVR 11112222, og sender derfor en forespørgsel afsted til samtykkesystemet, for at undersøge om samtykkerne allerede er afgivet. For at kunne anvende de samme samtykker på tværs af fagområder er der vedtaget en konvention om at alle fagsystemerne anvender strengen "CVR_" efterfulgt af virksomhedens CVR-nummer uden mellemrum som samtykkenøgle, når de efterspørger et samtykke for en virksomhed. Herved undgås det også at den samme virksomhed skal afgive det samme samtykke mere end én gang.

Samtykkesystemet slår samtykkenøglen op, og konstaterer, at der dels ikke er afgivet samtykke, dels ikke er oprettet en indhentning af samtykke for samtykkenøglen og samtykkerne B og C. Dette formidles til DMDB.

DMDB præsenterer i brugerfladen denne besked til SEGES medarbejderen, og spørger om indhentning af samtykkerne skal sættes i gang. Medarbejderen bekræfter dette.
Første trin i indhentning af samtykkerne er, at slå op hvem persondatainteressenterne er for den pågældende virksomhed. I diagrammet er ansvaret for at kunne svare på dette modelleret i et særskilt system, men det kunne også være implementeret som en del af DMDB, som i så fald ville overtage dets ansvarsområder.

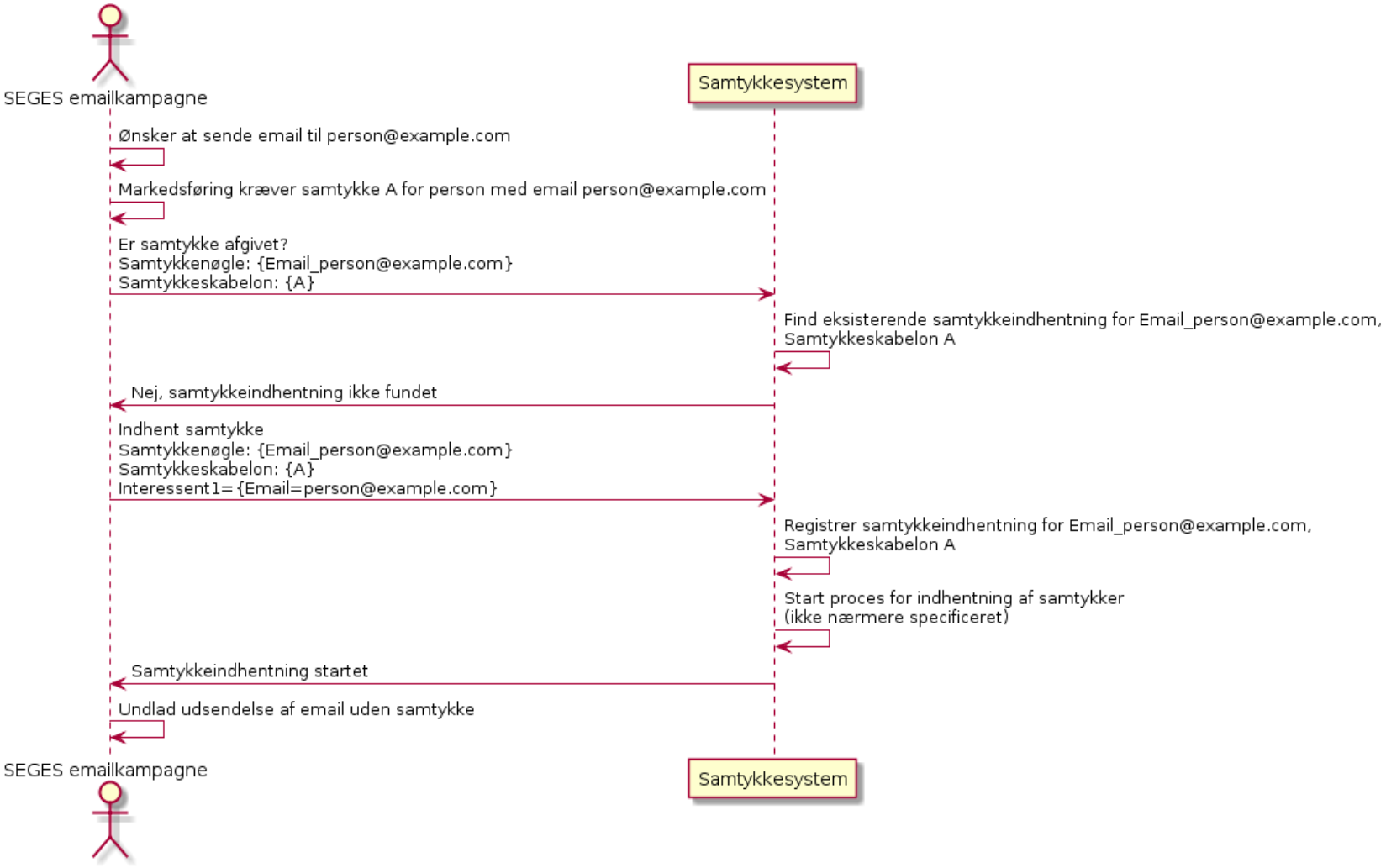
DMDB sender forespørgslen efter persondatainteressenter for CVR 11112222 til VirksomhedsPersondataInteressentregisteret, og det svarer tilbage med oplysninger om tre personer. VirksomhedsPersondata-Interessentregisteret står inde for at det kun er disse personer som virksomhedens data kan være henførbare til – typisk vil der være tale om ejerne.

Oplysningerne der forefindes for de tre personer er ikke ens. For den første kendes kun CPR, for den anden både CPR og en e-mailadresseadresse, og for den sidste kun en e-mailadresseadresse. Man kunne også forestille sig en situation, hvor kun en postadresse på enten bolig eller virksomhed var kendt for en eller flere af personerne. Disse personers oplysninger sendes til samtykkesystemet som en del af en forespørgsel på indhentning af samtykke for samtykkenøgle CVR_11112222.

Samtykkesystemet registrerer den nye indhentning i sin database. Til samtykkenøglen knytter den 3 registreringer af, at de medsendte personer skal afgive samtykkerne B og C. For at foretage registreringerne skal samtykkesystemet generere en nøgle for hver person, sammensat af den medsendte information om personen. Givet at de tilgængelige informationer kan ændre sig over tid, så kan der opstå en situation, hvor den samme person bliver afkrævet det samme samtykke mere end én gang, fordi nøglen har ændret sig. Dette kan kun undgås ved konsekvent brug af en entydigt, alment kendt nøgle, hvor CPR er eneste kandidat. Dette er sandsynligvis ikke muligt, men frekvensen af genopkrævning kan mindskes ved at prioritere brug af CPR som nøgle hvor det er tilgængeligt.

Når registreringen er foretaget, startes en manuel proces med at indhente samtykker. Samtykkesystemet stiller infrastruktur til rådighed for at afgive / registrere samtykkerne for de enkelte personer, eksempelvis via websider, hvor der kan foretages NemID signering af samtykketeksten, eller hvor SEGES medarbejdere kan registrere indscannede papirsamtykker. Som nævnt i afgrænsningen er formidlingen af forespørgslerne efter samtykkerne til de relevante persondatainteressenter ikke en del af samtykkesystemet. I stedet lægges samtykkeindhentningen i kø til manuel behandling, hvorefter det antages at nogen manuelt sørger for at notificere persondatainteressenterne, og få dem til at afgive eller afvise samtykkerne på websiderne til dette.

Det formidles til DMDB at samtykkeindhenting er startet, og DMBD videreformidler dette til SEGES medarbejderen. Endeligt afvises udførsel af analyse X, da de fornødne samtykker endnu ikke er til stede.



Figur 4 Eksempel på markedsføring

Sekvensdiagrammet i Figur 4 viser en automatisk proces omkring udsendelse af en e-mailadressekampagne til et antal brugere. For hver bruger skal det sikres at der er indhentet et samtykke A, hvor brugeren accepterer at modtage uopfordrede e-mailadresses fra SEGES.
Ligesom konventionen omkring samtykkenøglen for virksomheder giver mulighed for at fagsystemerne kan slå de samme samtykker op på tværs, så er der etableret en konvention om at personlige samtykkenøgler prefixes med ”CPR_” for samtykker hvor CPR er kendt, og ”E-mailadresse_” hvor e-mailadresse er kendt, og at henholdsvis CPR og E-mailadresse følger herefter.
Således bliver samtykkenøglen ”E-mailadresse_person@example.com”. Den sendes som en del af forespørgslen til samtykkesystemet, for at afklare om der er afgivet samtykke.

Samtykkesystemet konstaterer at samtykkenøglen ikke allerede findes, og parallelt med flowet i Figur 3 meldes dette tilbage til e-mailadressekampagnesystemet, der beder om indsamling af et nyt samtykke. Det antages at en e-mailadresseadresse kun har én ejer, og derfor kan e-mailadressekampagnesystemet umiddelbart sende en forespørgsel om indhentning af samtykke A for e-mailadresseadressen til samtykkesystemet. Med forespørgslen sender e-mailadressekampagnesystemet en enkelt interessent, identificeret på den e-mailadresse det ønsker at sende en markedsføringsmail til.

Resten af flowet forløber parallelt med det på Figur 3 illustrerede flow. Til sidst konstateres at der ikke er afgivet samtykke, hvorfor e-mailadresseen ikke afsendes.