NTNU
Det skapende universitet

Personvernsarkitektur

Hilde Visthoff Drange

Master i informatikk
Innlevert: Mai 2013
Hovedveileder: Guttorm Sindre, IDI
Medveileder: Carl-Fredrik Sørensen, NTNU IT

Norges teknisk-naturvitenskapelige universitet
Institutt for datateknikk og informasjonsvitenskap

Sammendrag

Personvern innenfor databehandling og informasjonsteknologi er et tema som opptar mange. Situasjonen i dag er at i enhver virksomhet finnes det mange systemer som inneholder til dels detaljerte opplysninger knyttet til personer og bedrifter. Dette kan være sensitive opplysninger som kan misbrukes til andre formål. Konsekvensen er at mange personer verken har oversikt eller tilgang til personopplysninger om seg selv, i tillegg til lite kontroll over hva opplysningene blir benyttet til.

I masteroppgaven har jeg gjennomført en kvalitativ og kvantitativ studie av kjennskap og holdninger til personvern, samt behov og muligheter for innføring og bruk av et felles personopplysningsregister ved utvikling av en personverninfrastruktur, -system og tjeneste, kalt IdMegler. IdMegler vil være et mellomvaresystem mellom tilgang til personopplysninger, arbeidsprosesser, saksbehandling og saksbehandlingsdata. Hovedoppgaven vil være å gi tilgang til koblinger mellom autoriserte klienter, samt logge tilgang og bruk. Gjennom litteraturstudie, dybdeintervjuer og spørreundersøkelser har jeg fått en innføring i dagens holdninger og arkitekturløsninger, i tillegg til fremtidige behov.

Studiet har hovedsaklig opptredd som et bindeledd mellom personvern og teknolgi og har bidratt ved å øke bevist- og synliggjøringen av hver enkelts rettigheter knyttet til personvern, og egne personopplysninger.

Hovedfokuset i oppgaven har vært å utrede en ny arkitekturløsning, IdMelger, som fremmer personvernet for den enkelte, samt en undersøkelse av studenters holdninger og kjennskap til personvern, for å avdekke om en mulig endring kan gjennomføres.

En løsning som IdMelger, og i samspill med et overordnet personopplysningsregister vil gi fordeler i fremtiden. Et stort personopplysningsregister kan være fordelaktig på tvers av bransjer og virksomheter, men en løsning som IdMegler kan gi sikkerhets- og tekniske utfordringer. Ved bruk av IdMegler vil det tilrettelegges for å unngå lovbrudd, enten med eller uten hensikt. Samt redusere faren for utro tjenere. En innføring av ny arkitektur vil også begrense spredningen av personopplysninger, øke kvaliteten på dem som er lagret og redusere konstnadene knyttet til vedlikehold av dem.

En av de største utfordringene ved innføringen av en ny arkitektur vil være å synliggjøre behovet for økt personvern for den enkelte bruker, samt behovet for innebygd personvern ved utvikling av nye løsninger. Gjennom nye løsninger må det tilrettelegges for å unngå lovbrudd som svekker personvernet, enten om lovbruddet er tilsiktet eller ikke. Det å heve kjennskapen og kunnskapen om personvern blant brukerne vil være en stor samfunnsmessig utfordring i fremtiden. Basert på de lave personvernskunnskapene i samfunnet er det gjennom oppgaven blitt satt fokus på hvordan personvernet for hver enkelt kan økes ved hjelp av tekniske løsninger og (tjeneste-orientert) arkitektur.

Gjennom en spørreundersøkelse holdt blandt studenter på NTNU, viser det seg at 65,8 % av de spurte studentene mener personvern er viktig for dem personlig, mens kun 24,2 % studenter har god kjennskap til personvern, og 8,7 % til personopplysningloven. Noe som viser at kjennskapen til både personvern og personopplysningsloven er lav. Samtidig forventer 76,3 % av de spurte studentene at personopplysningene deres ikke benyttes til andre formål enn det som er samtykket til.

IdMegler har i utgangspunktet ingen åpenbare risiki, og det er gjennomført en vurdering for hva bortfall av tjenesten kan medføre. IdMelger-arkitekturen kan benyttes og medfører økt personvern for den enkelte, ved bestemte forutsetninger.

Forord

Jeg visste ikke hva jeg gikk til da jeg startet på min masteroppgave i Informatikk ved Institutt for Datateknikk og Informasjonsvitenskap høsten 2012, men nå våren 2013 er den ferdig. Rapporten er resultatet av et års arbeid, men også et år med mange følelser og inntrykk, opp- og nedturer, samt mye ny kunnskap både innenfor Informatikk, men også innenfor andre fagområder. Selvdisiplinen og motivasjonen har i perioder blitt satt på prøve, men gjennom motiverende samtaler, veiledermøter og dybeintervjuer har oppgaven gitt meg mye gleder, utfordringer og verdifull kunnskap, både innenfor personvern, men også om meg selv.

Masteroppgaven har tittelen "Personvernsarkitektur", og omhandler personvern. Noe som er et dagsaktuelt og viktig tema for fremtiden, samt et tema som interesserer mange.

Jeg ønsker å takke veilederne mine Carl-Fredrik Sørensen og Guttorm Sindre for oppfølgning, innspill og støtte, samt verdifull og god hjelp gjennom hele prosessen. I tillegg ønsker jeg å takke familien min, da spesielt mamma, Elin Visthoff, for mange inspirerende diskusjoner, råd og motivasjon i tunge perioder.

Takk til Difi, Skatteetaten, Datatilsynet, Sparebanken 1-Gruppen og Statoil, for bidrag til datainnsamlinger gjort i forbindelse med studiet og masteroppgaven.

Hilde Visthoff Drange

Oslo, mai 2013

Innhold

Figurer

Tabeller

Forkortelser

ATS	Attributtbasert tilgangsstyring
Difi	Direktoratet for forvaltning og IKT
DLD	Datalagringsdirektivet
DSF	Det sentrale folkeregister
FAD	Fornyings-, administrasjons- og kirkedepartementet (Regjeringen)
FS	Felles Studentsystem (NTNU)
IKT	Informasjons- og kommunikasjonsteknologi
ISMS	Information security management system
IT	Informasjonsteknologi
LaPa	Layered Privacy Architecture
MDM	Master data management
NAV	Ny arbeids- og velferdsforvaltning
NOD	Nasjonal ordredatabase
NOKIOS	Norsk konferanse for IKT i offentlig sektor
NOU	Norges offentlige utredninger
NTNU	Norges teknisk-naturvitenskaplige universitet
PDCA	Plan-Do-Check-Act prosessmodell
PET	Privacy-enhancing technologies (Oversatt: Personvernsøkende teknologi)
PR	Partsregisteret (Skatteetaten)
RAIC	Redundant-Component Architectures
SAML	Security Assertion Markup Language
SERES	Semantikkregister for elektronisk samhandling
SOA	Service-oriented architecture (Oversatt: Tjenesteorientert arkitektur)
SSB	Statistisk sentralbyrå
UDI	Utlendingsdirektoratet

Begrepsordliste

Database	Strukturert samling av relaterte data
Elektronisk forvaltning (E-forvaltning)	Gjelder bruk av IKT i offentlig sektor, dvs i samband med myndighetsutøvelse, tjenesteyting og intern administrasjon.
Elektroniske tjenester	Manuelle arbeids- og kommunikasjonsprosesser som er digitalisert.
Enhetsregister	Enhetsregisteret har som hovedoppgave å samordne opplysninger om næringslivet og offentlige etater som finnes i ulike offentlige registre, og som er gjengangere på spørreskjemaer
Felles komponentforvaltere	Offentlige virksomheter som har overordnet og helhetlig ansvar for å utvikle og forvalte en eller flere felleskomponenter i tråd med overordnede styrings- og forvaltningsprinsipper.
Grunndata	Grunndata omtaler opplysninger om juridiske personer som registreres i Enhetsregisteret.
Grunndataregister	Et register bestående av grunndata, dvs. fortolkningsfrie data innenfor et bestemt fagområde, sektor eller etat. Norske grunndataregister er f.eks. Enhetsregisteret, Folkeregisteret.
Infrastruktur	Infrastruktur er det nett av faste anlegg som er grunnlaget for en virksomhet.
IT-Samordner	Samordningslinjen som har ansvaret for en helhetlig IT-samordning på tvers av alle sektorer.
IT-Arkitektur	"Reguleringsplan" for bruk av IT.
Offentlig forvaltning	Offentlig forvaltning består av offentlige virksomheter og ideelle organisasjoner som er kontrollert av myndighetene, og som ikke utøver sin virksomhet på et forretningsmessig grunnlag.
Personvern	Ivaretakelse av personlig integritet og personlige opplysninger.
Pearson (produkt-moment) korrelasjon	Måler samvariasjonen mellom to variabler ved å dele variablenes kovarians på produktet av variablenes respektive standardavvik.
Register	Et register er en samling av data om et bestemt emne og benyttes for å holde oversikt.
Taushetsplikt	Taushetsplikt er en plikt til å hindre andre å få adgang eller kjennskap til visse opplysninger.
Tjeneste	Noe som blir utført av en part for en annen part
Tjenesteeier	Alle offentlige virksomheter som har eller kan ha elektroniske tjenester ut mot innbyggere, næringsliv og andre offentlige virksomheter
Virksomhet	Virksomhet eller foretak er betegnelser for en organisasjon som produserer varer eller tjenester
Ytelsesnivå	Tilgjengelighet og responstid for en tjeneste

Del I

Personvern og arkitektur (Litteraturstudie)

1 Introduksjon

1.1 Innledning

> *Vi har alle noe vi ikke ønsker å dele med andre. Ikke fordi vi gjør noe ulovlig, eller har noe å skjule, men rett og slett fordi vi vil være i fred.*
>
> *Personvern handler om at man har grenser for hvor nært innpå seg man vil slippe andre. Retten til privatliv har en verdi som er vanskelig å måle. Mange av oss ser verdien først når personopplysninger er på avveie og vi opplever at vår integritet er truet*[1]*.*

Mangel på personvern

Norge preges av *systematisk mangel på sikring av personvernet* skriver den amerikanske organisasjonen *Electronic Privacy Information Center* og den engelske organisasjonen *Privacy International* som står bak rapporten *The Privacy and Human Rights Report* for 2007. Den viktigste faktoren som påvirker Norges plassering i rapporten er deling av opplysninger. Offentlige virksomheter deler opplysninger seg i mellom, uten at de eller den berørte blir varslet. Et eksempel er det nye NAV-registeret, EDAG (Elektronisk Dialog med Arbeidsgiver).

Et generelt problem er at det informeres for dårlig om hvilke personopplysninger som samles inn og hva de brukes til. Eksempelvis oppbevarer Norge i dag et asylsøkerregister med fingeravtrykk som er tilgjengelig for politiet ved kriminaletterforskning. Helt overordnet vil mangel på informasjon og oversikt gjøre det vanskelig for den enkelte å praktisere sine grunnleggende personvernrettigheter.

Ove Skåra, informasjonsdirektør i Datatilsynet mener nordmenn er for tillitsfulle overfor myndighetene og uttalte til Aftenposten.no i den forbindelse at;

> *Dette, kombinert med at vi er redde for blant annet kriminalitet, kan være noe av forklaringen på hvorfor Norge kommer så dårlig ut på personvern*[2]*.*

Deling av personopplysninger

Tidligere har staten og de offentlige virksomhetene vært sett på som den største trusselen mot et brudd på personvernet. I dag kan brukeren selv ses på som den største trusselen for eget personvern. Hovedsaklig gjennom deling av personopplysninger. Deling av personopplysninger kan føre til ukontrollert spredning, samt bruk av personopplysninger til andre formål enn det som var tiltenkt og samtykket til. Personopplysninger på avveie kan skape store samfunnsmessige problemer og konsekvenser for den enkelte det gjelder. I fremtiden vil det være viktig å ha fokus på innebygget personvern, samt holdninger og verdigrunnlag ved personvern.

Datatilsynet skriver i sin rapport *Personvern, trender og tendenser*[3]*, 2013*, at;

[1] Datatilsynet, Personvern på 1-2-3, www.datatilsynet.no, http://www.datatilsynet.no/personvern/, ukjent, 14.02.2013

[2] Aftenposten.no: Sørlie, Slakter personvernet i Norge, www.aftenposten.no, http://www.aftenposten.no/nyheter/iriks/article2190310.ece, 20.10.2011, 13.02.2013

[3] Datatilsynet, Personvern på 1-2-3, www.datatilsynet.no, http://www.datatilsynet.no/personvern/, ukjent, 26.04.2013

Å være tilstede på nett har blitt en nødvendighet - både praktisk og sosialt.

Sosiale medier

I noen tilfeller snakker vi om ukontrollert spredning av personopplysninger, i andre tilfeller deler man opplysningene selv. Ny teknologi bidrar til innsamling og kobling av personopplysninger i stor skala. Sosiale mediers fremtreden på midten av 2000-tallet har ført til stor økning i deling av informasjon på nett. Aldri før har det vært så stort fokus på personvern, og personvern har blitt noe enhver må forhold seg til. Sosiale medier åpner for mulighet til å kommunisere, skape og dele, men utfordrer også hver enkelts evne til å ha kontroll over egen informasjon[4]. Nordmenn er blandt de ivrigste i hele Europa på bruk av sosiale medier, med hele 80 % fordelt på Facebook, Twitter, LinkedIn og Instagram[5]. Av disse brukerne, har hele 93 % av befolkningen i alderen 15 - 29 år Facebook-profil, i tillegg har 54 % av befolkningen over 60 år bruker på et nettsamfunn[6].

Ved å publisere store mengder personopplysninger på nett, vil dette tilgjengeliggjøre store mengder informasjon og etterhvert digital historie, som igjen vil påvirke informasjonssikkerheten i samfunnet. Informasjonsikkerhet kan hovedsaklig deles i tre, tilgjengelighet, integritet og konfidensialitet (se kapittel 2.2, Informasjonssikkerhet), som er et av Regjeringens satsningsområder[7];

> *Dette betyr at informasjonen kun skal være tilgjengelig for de som har rett til å se den, den skal være der når den trengs og den skal være korrekt, fullstendig og autentisk.*

For å kunne tilfredstille kravene for informasjon bygges det på tre hovedprinsipper, *ansvar*; plikten til å handle etter samfunnets normer og igjen kunne forsvare sine handlinger, *likhet;* å ha samme status, kår og rettigheter som andre og *nærhet*; handler om å være innenfor kort avstand til noe. I dag anses tilgjenglighet som den viktigste faktoren innenfor informasjonssikkerhet.

Kjennskap til personvern

Den største personvernutfordringen er dårlig eller lite kjennskap til personvernslovingen og lagringsrutiner for personopplysninger. Mange virksomheter har problemer med å holde oversikt over hvilke personopplysninger de behandler, hvilke opplysninger som skal registreres og hvilke som ikke skal det. I tillegg lagres ofte opplysningene i ulike systemer og registre. Lagring av data er i dag rimelig, og det lagres stadig større mengder opplysninger i virksomhetene. Det kan dermed være vanskelig å etablere sletterutiner som tilfredstiller lovgivingen. Samtidig kan manglende sletterutiner ses som et resultat av vage lagringsrutiner. Manglende sletting fører ikke bare til et brudd på personopplysningsloven, men også en fare for at opplysningene blir brukt til andre formål enn opprinnelig tiltenkt. En annen stor personvernsutfordringer er knyttet til integriteten til lagrede

[4]Datatilsynet, Personvern: Tilstand og trender 2013, www.datatilsynet.no, http://www.datatilsynet.no/Global/04_veiledere/personvernrapport_tilstand_trender2013.pdf, 28.01.2013, 13.02.2013.

[5]Eurostat, Information society statistics, http://epp.eurostat.ec.europa.eu/, http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Information_society_statistics, 01.01.2012, 13.02.2013

[6]Datatilsynet, Personvern: Tilstand og trender 2013, www.datatilsynet.no, http://www.datatilsynet.no/Global/04_veiledere/personvernrapport_tilstand_trender2013.pdf, 28.01.2013, 13.12.2013.

[7]Regjeringen (FAD), Informasjonsikkerhet, www.regjeringen.no, http://www.regjeringen.no/nb/dep/fad/tema/ikt-politikk/informasjonssikkerhet.html?id=623457, ukjent, 14.12.2012

personopplysninger, da en del av opplysningene endrer seg over tid, men ikke blir oppdatert ved endring.

Identitetstyveri

Identitetstyveri eller ID-tyveri er en av verdens sterkest voksende kriminalitetsformer. Identitetstyveri definers som, *alle situasjoner hvor en person, uten samtykke enten:*

- *helt eller delvis er i stand til å utføre en eller annen form for uønsket pengeoverføring (transaksjon) i en annen persons navn,*
- *skaffer seg tilgang til ressurser tilhørende andre,*
- *urettmessig tilegner seg rettigheter som tilhører andre*[8].

Videre forklarer Datatilsynet begrepet identitestyveri i *Identitetstyveri, en utredning av Datatilsynet for Fornyings- og Administrasjonsdepartementet*[9],

> *Strengt tatt kan man ikke stjele andres identitet, men man forleder en tredjepart til å tro at man besitter en annens aktiva, rettigheter og plikter.*

Identitetstyven utnytter hull og mangler i den sosiale infrastrukturen og utgir seg for å være fornærmede. Normal tillit og troverdighet blir utfordret og offeret er i de fleste tilfeller helt ukjent for gjerningspersonen. Konsekvensene av et identitestyveri kan være store, og en tidlig forebygging kan føre til at identitetstyveri ikke utvikler seg til et alvorlig problem i Norge.

En navneliste på avveie kan skape større problemer enn først antatt. NRK skrev i april 2010 om at 38.000 personer hadde tilgang til navnelister over etterretningsansatte[10] og annen hemmeligstemplet informasjon. Personinformasjon om de ansatte var lagret direkte i NAV sitt Aa-registeret (Arbeidsgiver- og arbeidstakerregisteret). I utgangspunktet skal all informasjon om arbeidstakere og arbeidsgivere registreres her og annen unntaket er hemmligstemplet informasjon. Videre skrev Dagbladet august 2010 om 250.00 passnummer på avveie[11]. I forbindelse med Fotball-VM valgte en FIFA-ansatt å selge informasjonen på svartebørsen. I begge sakene er det høyrisiko for misbruk og utro tjenere, til tross for lukkede systemer, grunnet lett tilgjengelighet til lagret informasjon.

Digitaliseringsprogrammet

Regjeringen har lagt frem en handlingsplan, Digitaliseringsprogrammet, for hvordan man kan tilby bedre teknologiske løsninger som igjen skal føre til bedre personvern. Fornyings- administrasjons-

[8] Datatilsynet; Hvordan oppdage, forebygge og bekjempe ID-tyveri?, www.datatilsynet.no, http://www.datatilsynet.no/Sikkerhet-internkontroll/ID-tyveri/Oppdagem-forebygge-og-bekjempe-ID-tyveri/, 17.01.2012, 18.03.2013

[9] Datatilsynet, Identitetstyveri, en utredning av Datatilsynet for FAD, www.datatilsynet.no, http://www.datatilsynet.no/Global/04_analyser_utredninger/2009/Utredning%20om%20ID-tyveri.pdf, 30.01.2009, 14.02.2013.

[10] NRK: Ekroll og Døvik, 38.000 kan se navnelister over etterretningsansatte, www.nrk.no, http://www.nrk.no/nyheter/1.7101624, 29.04.2012, 14.12.2012

[11] Dagbladet: Sandli og Krokfjord, 250 000 passnumre på avveie, www.dagbladet.no, http://www.dagbladet.no/2010/08/19/nyheter/fifa/fotball-vm/svartebors/billetter/13009031/, 19.08.2010, 14.12.2012

og kirkedepartementetminister Rigmor Aasrud sa i forbindelse med Regjeringens lansering av Digitaliseringsprogammet i sin tale, *På nett med innbygerne*[12] at

> *Regjeringen tar sikte på at du som innbygger skal tilbys flere, bedre og smartere digitale tjenester. Offentlige tjenester fra ulike virksomheter skal kobles sammen i én og samme nettjeneste dersom tjenestene logisk hører sammen. Slik kan du få utført tjenester fra flere offentlige etater i ett og samme ærend* (Aaserud, 2012).

Videre la hun frem lovnader om å utvikle noen felles IT-løsninger som offentlige virksomheter skal benytte for å lage gode digitale tjenester.

> *Vi vil også videreutvikle Altinn, samt forbedre grunndataregistre om personer (Folkeregisteret, bedrifter (Enhetsregisteret) og eiendom (Matrikkelen) for felles bruk i det offentlige* (Aaserud, 2012).

Aasrud avsluttet talen med å vektlegge at det er viktig å bevare fokus på personvern og sikkerhet i løsningene som utvikles.

> *De felles IKT-løsningene i staten skal være effektive, robuste og ivareta sikkerheten, slik at opplysninger brukes til riktige formål og ikke kommer på avveie. Regjeringen vil legge frem nye nasjonale retningslinjer for å styrke informasjonssikkerheten* (Aaserud, 2012).

For å oppnå felles IKT-løsninger i det offentlige, må arkitekturen og oppbyggningen av den utredes og videreutvikles. Viktige prinsipper for arkitektur finnes nedfelt i St. meld. nr. 17 (2006-2007) avsnitt 7.3.2[13].

> *Den overordna IKT-arkitekturen i det offentlege skal vere fleksibel og tilpasningsdyktig, slik at den i størst mogeleg grad samspeler med dei IKT-arkitekturar som eksisterer innan einskildsektorar og den einskilde verksemda. Dei noverande systema er ofte verksamhetskritiske. Omstillingsarbeide må kunne skje under føresetnad av at løpande forvaltning og produksjon kan gå normalt. Føringane frå overordna IKT-arkitektur skal i minst mogeleg grad vere til hinder for endringar i verksemdenes oppgåveløysing og organisering*

[12] Rigmor Aasrud, På nett med innbyggerne, www.regjeringen.no, http://www.regjeringen.no/nb/dep/fad/aktuelt/taler_og_artikler/minister/taler-og-artikler-av-fornyings–og-kirke/2012/pa-nett-med-innbyggerne.html?id=678357, 13.04.2012, 15.11.2012

[13] Regjeringen: FAD, St.meld. nr. 17, Eit informasjonssamfunn for alle, www.regjeringen.no, http://www.regjeringen.no/Rpub/STM/20062007/017/PDFS/STM200620070017000DDDPDFS.pdf, 15.12.2006, 03.02.2013

Norge er i dag rangert som nummer fire på området for IKT-infrastruktur i verden[14]. Til tross for den høye rangeringen, har Norge utfordringer knyttet til arkitektur og mulighetene for innføring av overordnede prinsipper og felles retningslinjer for arbeid med IT i offentlig sektor. Datadirektivets årsmelding fra 2011, argumenterer for at veien fremover er å illustrere nytten av innebygget personvern, en konsekvensvurdering for personvernet, lovmessig forankring av personvernskonsekvenser og forskning på personvernfremmende teknologi. Dette konkluderes med følgende utsagn;

> *Jo mer kontroll brukeren selv har over løsningen og hva den registrer, jo mer personvernsvennlig er den* (Årsmelding Datatilsynet, 2011)[15].

Folkeregisteret; Innføring av nytt personnummer

Difi foreslår en løsning på bruk av felles komponenter gjennom rapporten, *Nasjonale fellekomponenter i offentlig sektor* (Difi, 2010), som støttes av Regjeringens fremleggelse av Digitaliseringsprogrammet, *På nett med innbyggerne*. Her foreslås det opprettelse og videreutvikling av grunndataregistre, eksempelvis Enhetsregisteret[16] og Folkeregisteret[17].

> *Behovet for grunndata på personinformasjonsområdet ivaretas i dag i utgangspunktet av Det sentrale folkeregister (folkeregisteret). Imidlertid vedlikeholder en del offentlige virksomheter også grunndata på personinformasjonsområdet i lokale registre* (Difi, 2010).

Dette fører til underbruk av folkeregisteret og igjen overbruk av lokale registere. Direkte bruk av folkeregisteret vil gi økt kvalitet og sikkerhetsmessige gevinster, samt redusert behove for vedlikehold av lokale registre. Det er i dag store offentlige virksomheter som baserer seg på folkeregisteret. Eksempelvis Nav og Lånekassen.

Videre kan innføringen av Det nye folkeregisteret og nytt personnummer i 2018 (se kapittel 2.3.1) være en mulighet for innføring av nye arkitekturløsninger, da det allerede kreves store endringer i allerede eksisterende systemer, hos nesten samtlige virksomheter og systemer.

DLD

En annen samfunnsmessig motivasjonen for problemstillingen er innføring av Datalagringsdirektivet[18], DLD, som vil kreve en omstruktuering av mange systemer for å muliggjøre retninglinjene og kravene direktivet setter.

---

[14] Næringslivets hovedorganisasjon, IKT-INFRASTRUKTUR, www.nho.no, http://www.nho.no/files/IKT-infrastruktur.pdf, ukjent, 06.11.2012

[15] Datatilsynet, Årsmelding 2011; Tendenser og utviklingstrekk, www.datatilsynet.no, http://www.datatilsynet.no/Om-Datatilsynet/Aarsmeldinger/Arsmelding-2011/3-Tendenser-og-utviklingstrekk-/, 27.02.2012, 03.09.2012

[16] Brønnøysundregistrene, Enhetsregisteret, www.brreg.no, http://www.brreg.no/registrene/enhet/, ukjent, 07.11.2012

[17] Skatteetaten, Folkeregister, www.skatteetaten.no, https://www.skatteetaten.no/Alt-om/Folkeregistrering/, ukjent, 07.11.2012

[18] Datatilsynet, Datalagringsdirektivet(DLD), www.datatilsynet.no, http://www.datatilsynet.no/Teknologi/Datalagringsdirektivet/Om-datalagringsdirektivet/, 08.02.2012, 16.11.2012

> *Når DLD trer i kraft, vil alle tele- og internettilbydere i Norge være pålagt å lagre trafikkdata, lokaliseringsdata og abonnementsdata som fremkommer ved bruk av telefoni, mobiltelefoni, bredbåndstelefoni, e-post og internettaksess i seks måneder. Det vil si opplysninger om hvem som kommuniserte med hvem, når kommunikasjonen fant sted, hvor de kommuniserende befant seg og hvilken kommunikasjonsform som ble benyttet* (Datatilsynet, 2012).

Formålet med direktivet er å oppdage, etterforske og bekjempe kriminalitet, men ny teknologi og mulighet for lagring av store mengder data over tid, fører til en rekke utfordringer. Dette er en utvikling som krever økt fokus på personvern og personvernmessige utfordringer en innføring av direktivet fører til[19].

1.2 Bakgrunn

Det er i dag en rekke problemer knyttet til databehandling, personvern og sikkerhet[20]. Personvern er et tema som opptar mange i forhold til lovgiving, teknologi, økonomi og politikk. Dagens systemer innenfor offentlige virksomheter lagrer til dels detaljerte opplysninger knyttet til personer og bedrifter. Opplysningene kan være sensitive og slik situasjonen er, kan de (mis)brukes til andre formål enn det som opprinnelig var gitt tillatelse til. Det finnes i dag et overordnet folkeregister, Folkeregisteret, men det tilbyr ikke tjenester som et personregister, noe som medfører at personregistrene som benyttes kan inneholde til dels motstridende informasjon, noe som kan gi dårlig kvalitet. Etterhvert som flere og flere opplysninger (personopplysninger) blir tilgjengeliggjort på nett, vil sikkerhetsrisikoen rundt dem øke.

Personvern handler i første omgang om retten til å bestemme over egne personopplysninger, men også individers rett til å påvirke bruk og spredning av personopplysninger om seg selv[21]. Dermed vil det være fordelaktig å håndtere og vedlikeholde personopplysninger i et eget register. Bruk av personopplysningene i registeret kan gjøres gjennom sporbare integrasjoner med systemet. For at personer skal ha tillit til systemet, er det viktig at opplysningene og saksbehandlingsdata blir lagret på en slik måte at de ikke kan misbrukes, samt at det er mulig å fjerne informasjon som ikke lenger er relevant. Andre motivasjoner for ny og forbedret arkitektur vil være lagring i skybaserte løsninger, samt oppfølging av DLD (Datalagringsdirektivet). Et felles og overordnet register for personopplysninger vil øke kvaliteten på (person)opplysningene, samt muliggjøre og forbedre prosesser rundt sikkerhet og vedlikehold.

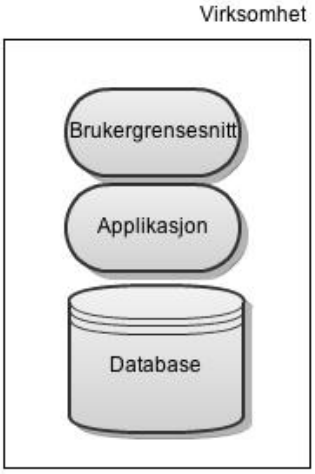
Mange av dagens arkitekturløsninger har ikke et fysisk skille mellom personopplysninger og saksbehandlingsdata. Et flertall av dagens systemer i offentlige virksomheter benytter selvstendige løsninger med egne brukergrensesnitt som bygger på applikasjoner og databaser, se Figur 1.1. Det er fordelaktig at fremtidige arkitekturstandarder tillater løskobling av saksbehandlingsdata fra per-

[19] Dagbladet: Krambe, DLD styrker personvernet, www.dagbladet.no, http://www.dagbladet.no/2010/11/25/kultur/debatt/debattinnlegg/dld/14428549/, 25.11.2010, 25.02.2013.

[20] Store Norske Leksikon, Databehandling: Personvern og sikkerhet, www.snl.no, http://snl.no/databehandling#menuitem8, ukjent, 21.08.2012

[21] Datatilsynet, Hva er Personvern?, www.datatilsynet.no, http://www.datatilsynet.no/personvern/Hva-er-personvern/, 25.11.2011, 30.08.2012

sonopplysninger, da disse ikke vil gi mening uten personkontekst og på den måte kunne øke det innebygde personvernet for den enkelte i IKT-løsningene.



Figur 1.1: Tre-lags arkitektur for virksomheter

Gjennom oppgaven presenteres en mulig tjeneste-orientert arkitektur, IdMegler, se også Kapittel 2.5, IdMegler. Bakgrunnen for IdMegler er ønsket om å opprette et klart skille mellom personopplysninger og saksbehandlingsdata for å øke personvernet for den enkelte person. Gjennom IdMegler ønskes det at hver enkelt person skal ha en viss kontroll og medinnflytelse over hvordan andre behandler opplysninger som angår en selv. Opplysningene skal ikke kunne benyttes til andre enn eksplisitt definerte formål. I tillegg skal det ikke samles inn flere data enn det som er strengt tatt nødvendig. Basert på dette kan det settes krav til at personopplysningene som samles inn er korrekte, fullstendige og oppdaterte.

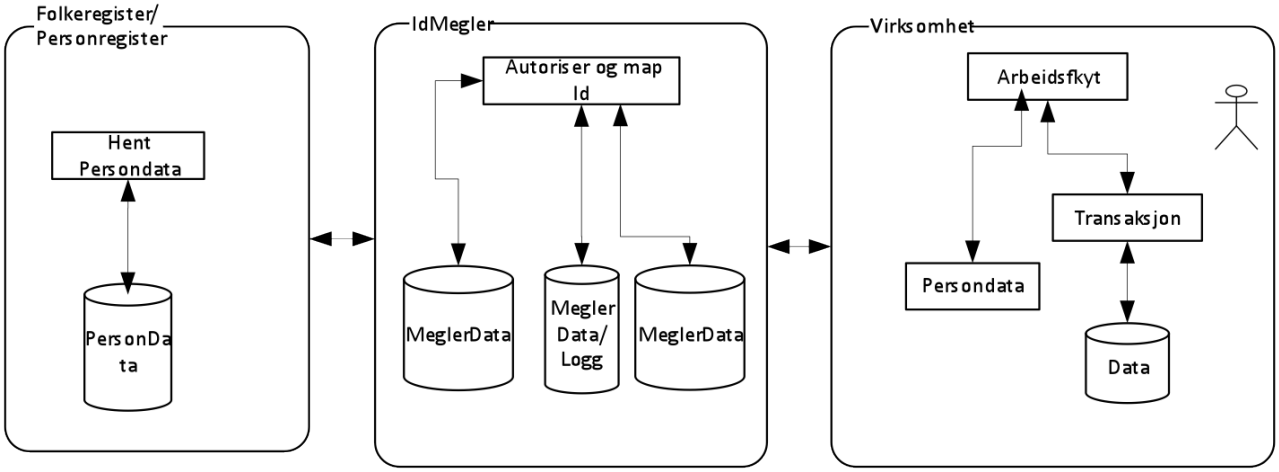
Gevinsten ved benyttelse av IdMegler vil være høyere kvalitet, redusert vedlikeholdsarbeid og økt sikkerhet på lagrede personopplysninger. I tillegg vil en person til enhver tid ha oversikt over personopplysninger lagret hos en virksomhet, det vil si kontroll av hvem eller hvilke virksomheter som bruker lagrede opplysninger, samt hva de blir brukt til.

Hovedrollen til IdMegler vil være å koble sammen saksbehandlingsdata (transaksjoner) og personopplysninger. Figur 1.2 viser IdMegler som et mellomvaresystem med spesifikke roller, som gir tilgang for autoriserte klienter for visning/kobling av person(opplysninger) mot saksbehandlingsdata. All saksbehandlingsdata relatert til personer lagres med nøkler tilgjengeliggjort gjennom IdMegler og benytter IdMegler for å sammenkoble informasjon ved hjelp av nøkkelmegling mellom virksomhet og personopplysningsregisteret.

For å sammenkoble informasjon (for eksempel objekter som har tilknyttning til personer) kan IdMegler benytte seg av pseudoID. Et pseudonym er et fiktivt navn påtatt for et bestemt formål som dekknavn for en person eller gruppe, som et alternativ til det orginale navnet. Dermed er en PseudoID en ID en selv tillegger seg og som ikke nødvendigvis er identisk med faktisk identitet[22].

[22]TU Dresden, Pfitzmann & Hansen, Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity

PseudoID kan knyttets med grunntaken til PET, ved at opplysninger som lagres er koblet til et pesudonym og ikke direkte kan kobles til en identifiserbar person. Bruk av pseudoID kan gi økt personvern ved at opplysninger er knyttet til et pseudonym og hindrer direkte identifisering av den opplysningen gjelder[23].



Figur 1.2: Arkitektur for IdMegler (Sørensen, 2011)

1.3 Problemstilling

I innledningen og bakgrunnen til oppgaven, gjengis grunnleggende strategier og målsetninger for en felles IT-arkitektur i offentlig sektor, med fokus på personvern. For å kunne oppnå disse, kreves et samarbeid mellom offentlige og private aktører, og en endring vil innebære store omlegginger av den eksisterende IT-arkitekturen. Omleggingen vil by på mange og tildels omfattende tekniske, økonomiske og politiske utfordinger.

Det er et behov for økt kvalitet og fokus på personvern ved innhenting, lagering og sletting av persondata, som beskrevet i bakgrunnen for oppgaven. Et felles register kan være med på øke kvaliteten på informasjon som ligger lagret, og redusere arbeidet og kostnadene ved vedlikehold av allerede lagrede personopplysninger.

Oppgaven vil fokusere på ønsket og behovet for et fellesregister eller felles folkeregister for personopplysninger i offentlige og private virksomheter, samt holdninger rundt en endring med medfølgende utfordringer. Oppgavens hovedproblemstilling er; *Det finnes ikke et felles register for personopplysninger* (Heretter; Personopplysningsregisteret). Dagens kilder til personopplysninger kan inneholde til dels motstridende informasjon.

Hovedmålet med oppgaven vil være å se på muligheten for å etablere en personvernsinfrastruktur, -system og -tjeneste. Dette kan oppnås gjennom et klart skille mellom bruk og selve opplysningene. Dette utdypes videre i forskningspørsmålene;

Management – A Consolidated Proposal for Terminology, http://freehaven.net/anonbib/cache/terminology.pdf, 06.12.2005, 29.04.2013.

[23]Regjeringen, FAD, Individ og integritet; Pseudonyme helseregistre, www.regjeringen.no, http://www.regjeringen.no/nb/dep/fad/dok/nouer/2009/nou-2009-1/27/2.html?id=542369, ukjent, 29.04.2013

1. *Hvordan kan en tjeneste-orientert arkitektur forbedre anonymifisering av personopplysninger i forhold til Personopplysningsloven? og dermed være bidragsyter til å bekjempe identitetstyveri? (FS1)*

2. *Hvilke teknologisk støtte/prosess har du som person i forhold til å hente ut/få innsyn i/slette personopplysninger om deg selv, lagret hos ulike virksomheter (på nett)? (FS2)*

3. *Er det mulig og hensiktsmessig å opprette en felles kilde til personopplysninger/ et felles folkeregister for personopplysninger? Hvor stor del av opplysningene som lagres er statiske? og igjen hvor mange av dem er knyttet til bruk? (FS3)*

4. *Hvem eier informasjonen som er lagret hos en virksomhet om en person? (FS4)*

1.4 Avgrensninger

En personvernsarkitektur dekker IKT-arkitektur, personvern og informasjonssikkerhet, fagområder som spenner bredt. Ved innførning av en ny akritektur vil det være tekniske, organisatoriske, juridiske, øknomiske og politiske utfordringer.

Norge har i dag et overordnet register i Folkeregisteret, som inneholder informasjon om nordmenn og andre bosatt og skattepliktig til Norge. Tilgang til Folkeregisteret er regulert av Folkeregisterloven, og forvaltes av Skattedirektoratet. Dermed vil det foreslås en ny arkitektur, IdMegler som tilbyr identitetsmegling og tilgang til personopplysninger.

1.5 Oppbygning

Del 1, Personvern og arkitektur

Kapittel 1, Innledning - en introduksjon til oppgaven. Kapittelet beskriver oppgavens bakgrunn og samfunnets behov med tilhørende utfordringer. I tillegg beskrives problemstilling, forskningsspørsmål, avgrensninger og oppbygging.

Kapittel 2, Litteraturstudie - er en innleding til personvern og ulike arkitekturløsninger. Kapittelet belyser generelle problemstillinger og forklarer begreper som informasjonsikkerhet, IKT-arkitektur, det sentrale folkeregister og IdMelger. Videre ser kapittelet på forskning som er gjort på fremtidige og eksisterende løsninger.

Del 2, Forskning

Kapittel 3, Forskning/Metode - er oppgavens forskningstilnærming. Kapittelet tar for seg valg av forskningsmetoder for å besvare problemstillingene, det vil si en begrunnelse for valg av spørreundersøkelse og dybdeintervju, inkludert utvikling av disse og datainnsamling. Videre ses det på måleproblematikk, validitet og realiabilitet.

Del 3, Analyse

Kapittel 4, Spørreundersøkelse - tar for seg analyse av innsamlet data for de tre spørreundersøkelsene. Spørreundersøkelsene blir analysert statistisk, og presentert i forhold til fagområder og tema. Kapittelet avsluttes med en overordnet oppsummering hvor det trekkes paralleller mellom de ulike spørreundersøkelsene.

Kapittel 5, Dybdeintervju - tar for seg analyse av dybdeinterjvuene, fra både offentlig og privat sektor. Dybdeintervjuene presenteres gjennom en tematisk sammenfatning og videre gjennom ulike perspektiver på IdMelger. Kapittelet avsluttes med en overordnet oppsummering av de ulike tema i forhold til sektor og virksomhet.

Del 4, Avslutning

Kapittel 6, Diskusjon - er en diskusjon og oppsummering av resultater og funn fra litteraturstudie, forskning- og analysekapittelet og en avslutning av oppgaven. Kapittelet presenterer og argumenterer også for ulike muligheter og konklusjoner for forskningsspørsmålene og problemstillingen.

Kapittel 7, Konklusjon - er en besvarelse av forskningsspørmålene og tilhørende problemstilling er basert på diskusjon i kapittel 6.

Kapittel 8, Videre arbeid - tar for seg videre arbeid med oppgaven. Muligheten for å utvikle IdMelger og hva som kreves for dette, på det funksjonelle og tekniske plan.

Kapittel 9, Referanser - presenterer akademiske referanser og kilder benyttet gjennom oppgaven, hovedsaklig i forbindelse med litteraturstudiet.

Del 5, Appendiks

Vedlegg A; En beskrivelse av IdMegler
Vedlegg B; Spørreundersøkelsene
Vedlegg C; Intervjuguidene.

2 Litteraturstudie

Kapittelet beskriver dagens IKT-arkitekturløsninger og systemer, samt styrker og svakheter ved disse. Videre forklares personvern med utgangspunkt i Personopplysningsloven og mulige system- og personvernsarkitekturer. Her diskuteres bruk av felleskomponenter i offentlige virksomheter og det blir presentert konkrete løsninger som benyttes i dag. Det tas utgangspunkt i offentlige virksomheter, selv om mange av prinsippene og problemstillingene kan være aktuelle også for private virksomheter.

2.1 Personvern

Personvern blir forbundet med interessen til å kontrollere formidling og bruk av opplysninger som angår en selv, når og til hvem, til hvilket formål og hvem opplysningene videreformidles til (Bing, 1991). Personvern kan dermed beskrives som et komplekst begrep og benyttes på ulike måter, i ulike sammenhenger[24] og kan lett knyttes til personopplysninger.

Behandling av personopplysninger reguleres gjennom Personopplysningsloven(Justis- og politidepartementet, 2000)[25]. Formålet med loven beskrives i § 1.

> *Formålet med denne loven er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger.*
>
> *Loven skal bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger.*

Videre definerer § 2, første, andre og tredje ledd henholdsvis personopplysninger, behandling av personopplysninger og personregistre.

> *1) personopplysning: opplysninger og vurderinger som kan knyttes til en enkeltperson*
> *2) behandling av personopplysninger: enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter.*
> *3) personregister: registre, fortegnelser m.v. der personopplysninger er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen.*

Deretter følger beskrivelse av hva som regnes som sensitive personopplysninger i § 2, åttende ledd.

> *Sensitive personopplysninger: opplysninger om*
> *a) rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning,*

[24] Regjeringen (FAD), Hva er Personvern?, www.regjeringen.no, http://www.regjeringen.no/nb/dep/fad/tema/personvern/hva-er-personvern.html?id=448290, ukjent, 13.09.2012

[25] Lovdata, LOV 2000-04-14 nr 31: Lov om behandling av personopplysninger (personopplysningsloven), www.lovdata.no, http://www.lovdata.no/all/hl-20000414-031.html, 14.04.2000 ,12.09.2012

b) at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling,
c) helseforhold,
d) seksuelle forhold,
e) medlemskap i fagforeninger.

Personopplysningsbegrepet er godt forankret i lov, fagmiljøer og fovaltning. Mange virksomheter lagrer i tillegg til personopplysninger også andre opplysninger. Disse kan være taushetsbelagt etter Ligningsloven (Finansdepartementet, 1980)[26] §3 punkt 13 (gjelder ligningsområdet) og Forvaltningsloven[27] §13. Taushetsplikten (se Begrepsordliste) innebærer blant annet at opplysninger skal skjermes med unntak av de som har tjenestelig behov for dem og de opplysningene omhandler. Samtidig finnes de en del unntak i regelverket som gir andre hjemmel til opplysninger som er taushetsbelagt.

Kapittel to og tre i Personopplysningsloven tar for seg regler for og informasjon om behandling av personopplysninger. Videre utdyper § 18, første ledd i Personopplysningsloven hvert enkelt individs rett til innsyn i lagrede personopplysninger.

Enhver som ber om det, skal få vite hva slags behandling av personopplysninger en behandlingsansvarlig foretar.

Grunnlaget for et av de viktigste prinsippene ved Personopplysningsloven, er at hver enkelt person skal kunne bestemme over egne personopplysninger. Dette beskriver behovet for privatliv, personlig integritet og kvalitetsnivå på opplysningene som lagres (Bråten, 2008). Personvernkommisjonens utredning: *NOU 2009: 1. Individ og integritet: Personvern i det digitale samfunnet*[28] underbygger dette;

Personvern dreier seg om ivaretakelse av personlig integritet, ivaretakelse av enkeltindividues mulighet for privatliv, selvbestemmelse og selvutfoldelse.

Schartum og Bygrave argumenterer i boken *Personvern i informasjonssamfunnet (*Schartum, 2004*),* for at det er umulig å definere personvern helt klart, fordi begrepet betegner "interesser" og "verdier". Utsagnet begrunnes ved at personvern har bredt bruksområde og benyttes i mange forskjellige sammenhenger. Personverninteresser beskrives som synlig og aktualiserte problemstillinger, mens verdier betegner personvernsinteresser som er aktuelle i dagens diskusjoner. Dermed er det viktig å se personinteresser opp mot personvernlovgivingen, en beskrivelse av hvilke interessekonflikter og interesser personvernet gjelder (Bråten, 2008).

[26]Lovdata, LOV-1980-06-13 nr 24: Lov om ligningsforvaltning (ligningsloven), www.lovdata.no, http://www.lovdata.no/all/nl-19800613-024.html, 13.06.1980 ,23.01.2013
[27]Lovdata, LOV-1967-02-10: Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven), www.lovdata.no, http://www.lovdata.no/all/nl-19670210-000.html, 10.02.1967 ,23.01.2013
[28]Regjeringen (FAD), NOU 2009: 1 Individ og integritet - Personvern i det digitale samfunnet, www.regjeringen.no http://www.regjeringen.no/nn/dep/fad/Dokument/NOU-ar/2009/nou-2009-1.html?id=542049, 13.01.2009, 13.09.2012

2.1.1 Personvern i praksis

Det kan utifra nyhetsbildet leses om jevnlige brudd på personvernet og Personopplysningsloven. Eksempelvis kan man se på Skatteetaten og Lånekassens bruk av Google Analytics[29]. Virksomhetene benyttet analyseverktøyet for måling og analyse av besøkstrafikk. Problemet var at ingen av virksomhetene kunne svare for om IP-adressene som ble hentet inn av analyseverktøyet ble anonymisiert eller benyttet til andre analyseformål enn tiltenkt. Et annet eksempel kan hentes fra tilgjengeliggjøring av skattelistene i 2012. Ved innlogging på Altinn fikk over 2000 personer tilgang til Kenneth sin side[30] og muligheten for å se hans private personopplysninger. Brudd på Personpplysningsloven finnes også i helsebransjen, med innsyn og spredning av pasientjournaler[31].

Et brudd på Personopplysningsloven kan defineres som all bruk av personopplysninger uten gyldig behandlingsgrunnlag. Et lovbrudd kan være tilsiktet, altså kriminelt, eller et uhell. Det kan i tillegg være ulike (personlige) interesser og syn, etisk eller juridisk, bak et lovbrudd. Eksempelvis kan et brudd på Personopplysningsloven være lekking eller gjenbruk av innsamlede personopplysninger. Innsamlede personopplysninger, lagret i en virksomhets database, er ikke en virksomhet sine eiendeler, men informasjon samlet inn ved samtykke til bruk ved et bestemt formål[32].

Som beskrevet i kapittel 2.1, Personvern, er behandlig av personopplysninger regulert av Personopplysningsloven (Justis- og politidepartementet, 2000). Her stilles krav til behandling og at hver enkelt person har mulighet til innsyn i personopplysninger lagret om seg selv. Personopplysningsloven er lite konkret, og i mange tilfeller, vil det være vanskelig å gjøre opp for skaden som har skjedd, ved bruk av fengselstraff eller bøter. Dette fører til at det benyttes skjønn ved mange domsavgjøreser og at det kun er brudd på et utvalg av bestemmelsene i loven som kan straffes (Regjeringen: Overtredelsesgebyr, 2008). Det vanligste er å straffe lovbrudd med bøter, men § 48, første ledd i Personopplysningsloven, beskriver en strafferamme på fengselstraff på inntil ett år ved forsett eller grov uaktsomhet, og fengselsstraff inntil tre år ved særdeles skjerpende omstendigheter[33].

2.1.2 Personvern og teknologi

PET (*Privacy-enhancing technologies*) blir oversatt til Personverns -økende eller -fremmende teknologi og er en kobling mellom teknologi og personvern (Regjeringen, Personvernøkende teknologi og identitetsforvaltning, 2009). Begrepet oppstod som følge av det stadig økende problemet datakriminalitet, og skal begrense muligheten for identifisering av personopplysninger. Dette er mål som gjenspeiles i Personopplysningsloven(Justis- og politidepartementet, 2000) og *NOU 2009: 1. Individ og integritet: 4. Personvernøkende teknologi og identitetsforvaltning.*

[29]Digi: Jørgenrud, Ulovlig å bruke Google Analytics, www.digi.no, http://www.digi.no/900690/ulovlig-aa-bruke-google-analytics, 20.08.2012, 21.08.2012

[30]Aftenposten: Eggesvik, 2000 personer kan ha sett Altinn-siden til Kenneth, www.aftenposten.no, http://www.aftenposten.no/nyheter/iriks/2000-personer-kan-ha-sett-Altinn-siden-til-Kenneth-6789737.html#.T2pQ7tWvO8A, 21.03.2012, 21.08.2012

[31]Nettavisen: Johansen, Ansatte snoket og spredde pikante pasientopplysninger, www.nettavisen.no, http://www.nettavisen.no/nyheter/article3350607.ece, 06.03.2012, 28.08.2012

[32]Norsk senter for informasjonssikring: Aanensen, Bruk og misbruk av personopplysninger, www.idtyveri.no, http://www.idtyveri.info/index.php?option=com_content&view=article&id=39:bruk-og-misbruk-av-personopplysninger&catid=8:beskytt-personopplysninger&Itemid=12, ukjent, 17.09.2012

[33]Lovdata, LOV 2000-04-14 nr 31: Lov om behandling av personopplysninger (personopplysningsloven), www.lovdata.no, http://www.lovdata.no/all/hl-20000414-031.html, 14.04.2000 ,12.09.2012

> *Fokuset på identitet kan forklares ved at personverninteresser ikke gjør seg gjeldende dersom den opplysningene gjelder ikke kan identifiseres* (Regjeringen, Personvernøkende teknologi og identitetsforvaltning, 2009).

Ved å skille identitet og personverninteresser, vil det forsterke den enkeltes personvern. Eksempelvis kan et skille mellom saksbehandlingsinformasjon, som for eksempel transaksjoner og personopplysninger, vanskeliggjøre misbruk og spredning av persondata og aktiviteter knyttet til personene.

Hovedmålene ved *PET* er å tilrettelegge for overholdelse av lovene og retningslinjene knyttet til Personopplysningsloven, samt øke kvaliteten på lagret personinformasjon. Tilrettelegging krever fokus på minimalisering av lagret personinformasjon, og personlig kontroll over data (van Blarkom, 2003). Innføring av *PET* vil føre til samfunnsmessige fordeler, blandt dem økt sikkerhet og lavere risiko for datakriminalitet og igjen lovbrudd, som fører til økt tillit blant brukerne av ulike systemer.

Innebygget personvern

Innebygget personvern handler om evnen til å ivareta personvernet i alle utviklingsfaser av nye systemer. Ved utvikling av nye systemer er det viktig å finne balansen mellom personvern, brukervennlighet og tilgjengelighet. Datatilsynet skriver på sin hjemmeside om *7. steg til innebygget personvern*[34]*;*

1. Vær i forkant, forebygg fremfor å reparere - Det er viktig å vurdere risikoene for personvernet så tidlig som mulig i utviklingsprosessen.
2. Gjør personvernet til standardinnstilling - Standardinnstillinger er førende for hvordan systemet blir.
3. Bygg personvern inn i designet - Implementer personvern som en del av kjernefunksjonaliteten.
4. Skap full funksjonalitet: Både-og - Det er viktig å ivareta både brukerens personvern og egne behov.
5. Ivareta informasjonsikkerheten fra start til slutt - Personopplysninger skal sikres mot uatorisert tilgang, endring, ødeleggelse og spredning.
6. Vis åpenhet - Åpenhet om hvordan systemet fungerer og hvordan personvernet blir ivaretatt.
7. Respekter brukerns personvern - Det er viktig å gi brukernes personvern høy prioritet.

[34]Datatilsynet, 7. steg til innebygget personvern, www.datatilsynet.no, http://www.datatilsynet.no/Teknologi/Innebygd-personvern/, 19.04.2013, 27.04.2013.

2.1.3 Personvern og tilsyn

Det finnes i dag et omfattende lovverk for å regulere og behandle personopplysninger. For å følge opp lovverket og gjennomføre tilsyn er det opprettet egne forvaltningsorgan for de ulike bransjene. Forvaltningsorganene har som oppgave å administrere det offentlige regelverket innenfor fagområdet. Det mest kjente forvaltningsorganet er Datatilsynet, men også Post- og teletilsynet, Helsetilsynet og Arbeidstilsynet gjennomfører tilsyn.

- Post- og teletilsynet, *er det sentrale utøvende tilsyns- og kontrollorgan på områdene for post og elektronisk kommunikasjon i Norge*[35]. Post- og teletilsynet fører tilsyn, tar stikkprøver, utfører målinger og gjennomfører annen kontroll av nettet. De kan også kreve at virksomheter etablerer systematisk internkontroll slik at forskriften blir oppfylt[36].

- Statens helsetilsynet , er underlagt Helse- og omsorgsdepartementet og overordnet tilsynsmyndighet for sosiale tjenester som Nav og barnevern-, helse- og omsorgstjenester i Norge[37].

- Arbeidstilsynet, *er en statlig etat, underlagt Arbeidsdepartementet.* Arbeidstilsynets hovedoppgave er å føre tilsyn for å kontrollere at virksomhetene følger arbeidsmiljølovens krav[38].

Forvaltningsorgangene benytter seg av ulike arbeidsmetoder for å gjennomføre kontroll, alt fra områdeovervåkning, (ikke) planlagt tilsyn, i forbindelse med klager på tjenester og ved bruk av funn og erfaringer.

Personvern over landegrenser

Med økende bruk av outsourcing, nettsky-lagring og sosiale medier, øker også overføringen av personopplysninger over landegrenser. Dette byr på utfordringer i forbindelse med personvernslovgiving. I den forbindelse er det utviklet en internasjonal lov Safe Harbor som regulerer overføring av personopplysninger fra et EU/EØS-land til USA.

Safe Harbor prinsippene

Safe harbor er en særavtale mellom EU og USA som regulerer overføring av personopplysninger[39]. Loven oppstod som et resultat av innføringen av EUs datadirektiv (Directive 95/46/EC) i 1998, som forbyr overføring av personopplysninger til land som ikke følger EU sine regler for personvern. Da USA ikke er et EU/EØS-land forbyr direktivet overføring av personopplysninger fra et EU/EØS-land til USA, dersom ikke personen det gjelder samtykker til informasjonsdelingen.

[35] Regjeringen; Samferdselsdepartementet, INSTRUKS FOR POST- OG TELETILSYNET, www.regjeringen.no, http://www.regjeringen.no/upload/SD/Vedlegg/etatsinstrukser/instruks-postogteletilsynet-12062009.pdf, 12.06.2009, 27.04.2013

[36] Lovdata, FOR 1997-12-05 nr 1259: Forskrift om offentlig telenett og offentlig teletjeneste (offentlignettforskriften), www.lovdata.no, http://www.lovdata.no/for/sf/sd/xd-19971205-1259.html, 05.12.1997, 27.04.2013

[37] Helsetilsynet, Tilsyn, www.helsetilsynet.no, http://www.helsetilsynet.no/no/Tilsyn/, ukjent, 27.04.2013

[38] Arbeidstilsynet, Organisering, www.arbeidstilsynet.no, http://www.arbeidstilsynet.no/om/index.html?tid=207114, ukjent, 27.04.2013

[39] U.S. Companies Export, Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks, www.export.gov, http://export.gov/safeharbor/index.asp, 04.11.2012 ,23.04.2013

Lovgivingen er relevant i forhold til lagring av informasjon og data i skyen, ved bruk av amerikanske programmer som oppbevarer personopplysninger. F.eks. Facebook.

2.1.4 Personvern og forretning - Salg av personopplysninger

> *Enkel tilgang til store mengder personopplysninger, mulighet for rimelig lagring og fremvekst av nye analyseteknikker, driver også frem nye forretningsmodeller og virksomheter* (Årsmelding, 2011).

Ulike bransjer og virksomheter oppbevarer og lagrer personopplysninger om brukere av systemene og tjenestene de tilbyr. Dermed kan personopplysninger føre til forretningsmessige utfordringer, både i forhold til salg, men også markedsføring. Direkte salg av personopplysninger er ulovlig og regulert av Personopplysningsloven, men behandlet personinformasjon i form av statistikk og analyser er tildels lovlig å selge, dersom opplysningene er anonymisert.

Et eksempel kan hentes fra bankene, de har informasjon om alle transaksjonene kundene gjennomfører. Dette kombinert med personopplysninger, er verdifull informasjon i markedsføring. Annen verdifull informasjon er kjøpshistorikk, tidsserier, oppførselsdata, tekst og nettverksdata. Samtidig benyttes personopplysningene for å bekytte brukerne mot datakriminalitet. Dette gjøres ved å se brudd på bruksmønstre.

En ny arkitektur alá IdMegler, kan bidra til å gjøre det vanskeligere å koble informasjon, og dermed få nyttige og verdifulle statistikker og analyser som kan selges. Dette medfører høyere personvern og en sikrere lagring av personopplysninger for brukere av systemer. Dette vil gjøre salg- og markedsføringsbransjen smalere, siden salg av personopplysninger er avhengig av et høyt kvalitetsnivå og ikke minst konsistens på opplysningene som selges.

Google

Google er først og fremst kjent som en verdensomspennende søketjeneste og søkemotor. Målet deres er å organisere all informasjon i verden og gjøre den universelt tilgjengelig og nyttig. Dette skal Google oppnå gjennom stort fokus på brukeropplevelsen og på å gjøre den best mulig[40].

Google har gjennom de siste årene blitt kjent for å samle inn store mengder data og personopplysninger for bruk og salg mot markedsføring og reklame. Dette er deres desidert største inntektsskilde[41]. Google skriver i sine egne personverns retningslinjer at de gjennom informasjonsdeling ønsker å forbedre sine egne systemer og løsninger[42];

[40] Google, Om google, www.google.no, http://www.google.no/intl/no/about/, ukjent, 08.03.2013

[41] Teknofil; Nilsen, Google vokser i et utrolig tempo, www.teknofil.no, http://www.teknofil.no/artikler/googles_eventyrlige_vekst_fortsetter/100151, 18.07.2011, 10.03.2013

[42] Google, Retningslinjer og prinsipper, www.google.com, http://www.google.com/intl/no/policies/privacy/, 27.07.2012, 08.03.2013

Dette omfatter blant annet at vi viser deg mer relevante søkeresultater og annonser, hjelper deg å komme i kontakt med folk og at vi gjør det enklere og raskere å dele med andre.

Google samler inn informasjon brukerne gir dem gjennom bruk av tjenestene deres, i tillegg til enhets-, logg- og posisjonsinformasjon, samt informasjonskapsler og anonyme identifikatorer. Informasjonen benyttes til å levere, vedlikeholde, beskytte og forbedre tjenestene, i tillegg til å utvikle nye tjenester. Brukerne blir også tilbudt informasjon tilpasset innhold, og mer relevante søkeresultater og annonser.

Google har tilgang til store mengder data og i dagens samfunn har *Big data* blitt kjent som en samlebetegnelse for all informasjon som genereres på nett. *Big Data* refererer til datasett som er så enorme at de ikke kan analyseres ved hjelp av tradisjonelle databaseverktøy[43]. Det er ikke mengden data som er bakgrunnen for uttrykket, men det at dataene er samlet fra mange ulike kilder og analysert i den sammenheng. Hovedfordelen ved systematisering av Big data er at flere av brukerne får tilgang på mer data, av relevant art, som kan gi dem ny innsikt raksere, slik at de kan ta både raskere og bedre beslutninger. Et problem med Big data er at det ofte blir lettere å vite hvem personer, f.eks. i sosiale medier, noe som utgjør en stor personvernutfordring. En annen stor sårbarheten i Big data systemer er ustrukturerte data; mengden data vokser uten at virksomheten klarer å avgrense eller bruke dataene.

I noen tilfeller velger bedrifter å gjøre analyser på kundenivå i forbindelse med risiko, avgang og produktaffinitet, til tross for at dette ikke er lovlig (dersom ikke kundeinformasjon er anonymifisert). Data som benyttes er ofte begrenset til det som eksplisitt finnes om kunden, i tilegg til aggregert informasjon om hvordan kunden oppfører seg. En annen stor kilde til kunnskap rundt en person/kunde er transaksjonshistorikk. Ved analyse av transaksjonsinformasjon kan en få innsikt i kundens kjøpshistorikk, tidsserier, oppførselsdata og nettverksdata. Kobling av denne typen informasjon er en trussel for personvernet og en sårbarhet i Big-data systemer.

Facebook

Facebook er det desidert største sosiale nettverket i Norge - 79 % av kvinnene og 72 % av mennene er medlem[44].

Facebook er ikke bare stort i Norge og kan på verdensbasis med sine 800 millioner brukere, ses på som verdens største nettsamfunn. Det vil også si en lagring av 800 millioner brukerens personopplysninger.

Facebok skrev i september 2011, et brev[45] til Bjørn-Erik Thon, direktør i Datatilsynet, og som

[43] McKinsey Global Institute, Big Data: The next frontier for innovation, competition, and productivity, June 2011, 29.04.2013

[44] Datatilsynet, Personvern: Tilstand og trender 2013, www.datatilsynet.no, http://www.datatilsynet.no/Global/04_veiledere/personvernrapport_tilstand_trender2013.pdf, 28.01.2013, 10.03.2013.

[45] Datatilsynet; Facebook, Facebook´s Respons to Questions form the Data Inspectorate of Norway, www.datatilsynet.no, http://www.datatilsynet.no/Global/english/Facebook_questions_answere2011.pdf, 01.09.2011, 10.03.2013.

et svar på rapporten *Social Network Services and Privacy*[46], at Facebook regner navn, profilbilde, nettverk, brukeridentifikasjon og -navn som offentlig tilgjengelig informasjon. Derimot regnes ikke adresse, mailadresse og fødselsdato som offentlig informasjon, og vil dermed heller ikke bli delt med andre virksomheter. Facebook skriver videre i brevet at de kun deler begrensede sett med data, regnet som offentlig informasjon, med troverdige partnere i et kontraktsforhold med dem. Informasjon kan også benyttes mot reklame og igjen for å nå Facebook sitt mål, tilby en fri, global plattform for å knytte målrettede og relevante annonser basert på brukerprofilenes informasjon mot brukerne. Her legges det sterk vekt på at ingen brukerinformasjon deles med annonsører.

2.1.5 Relaterte begreper

Personvern er multidimensjonal, elastisk og dynamisk, noe som medfører en mengde overlappende begreper som ikke må forveksles. Konfidensialitet, hemmeligholdelse, sikkerhet, anonymitet og etikk er ikke personvern (Smith, 2011).

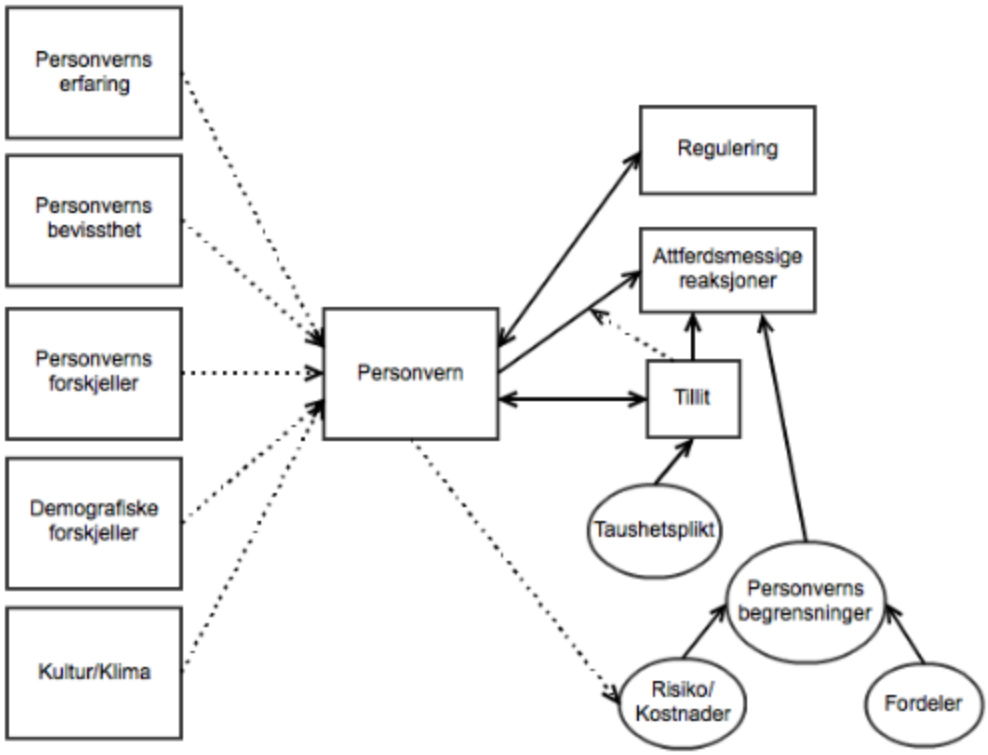
- *Anonymitet:* Er muligheten til å skjule en persons identitet. Anonymitet eksisterer når noe opptrer på en måte som begrenser muligheten til identifikasjon av andre. Begrepet er ofte formet av PET teknologiens muligheter, se kapittel 2.1.2. Anonymitet og personvern er interralterende.
- *Etikk:* er den systematiske refleksjon over egen og andres moral. Personvern kan tolkes fra mange etiske perspektiv.
- *Hemmeligholdelse:* Handler om å holde tilbake informasjon. Personvern har et behov for å skjule personopplysninger, men hemmeligholdelse handler om å skjule mye mer enn personopplysninger.
- *Konfidensialitet:* Handler om nøyaktighet og presisjon. Det vil si kontrollert frigjøring av personopplysninger beskyttet av en informasjonvokter og underlagt en avtale som begrenser spredning og bruk.
- *Sikkerhet:* Et vanlig problem er manglende forståelse av hvordan personvern og sikkerhetsproblemer er relatert;

  > *Security is necessary for privacy, but security is not sufficient to safeguard against subsequent use, to minimaize the risk of... discloseure, or to reassure users* (Ackerman, 2004).

Oversatt vil det si at sikkerhet er nødvendig for personvern, men sikkerhet kan ikke beskytte mot misbruk eller minske risikoen for det. Det er tre spesifikke mål knyttet til informasjonssikkerhet, nemlig integritet, konfidensialitet og tilgjengelighet.

[46]Datatilsynet; Årnes, Social Network Services and Privacy, www.datatilsynet.no, Social Network Services and Privacy, 15.04.2011, 10.03.2013

Figur 2.1 gir et inntrykk av forholdet mellom personvern og de andre faktorene. Figuren viser en APCO macro modell, (Antecedents, Privacy Concerns, Outcomes). Til venstre vises de ulike faktorene. Disse tilføres personvernegenskaper og basert på disse blir det gjort endringer før resultatet blir presentert.



Figur 2.1: Illustasjon (oversatt til norsk) av personvern og relaterte begreper (APCO-modell) (Smith, 2011)

2.2 Informasjonssikkerhet

> *Informasjonssikkerhet i henhold til Personopplysningsloven, handler om å sikre Personopplysningenes konfidensialitet, tilgjengelighet, integritet og kvalitet*[47].

Infomasjonssikkerhet er en avveining i forhold til de fire faktorene *konfidensialitet, tilgjengelighet, integritet* og *kvalitet*. *Konfidensialitet* handler om nøyaktighet og presisjon, begrenset tilgang til informasjon basert på autorisasjon på personer og prosess. *Tilgjengelighet* handler om muligheten for kommunikasjon mellom to eller flere parter. *Integritet* betyr at informasjon ikke skal være endret eller skadet og at *kvaliteten* skal være tilfredstillende.

[47]Store Norske Leksikon, Informasjonssikkerhet, www.snl.no, http://snl.no/informasjonssikkerhet, ukjent, 05.09.2012

Datatilsynet definerer informasjonsikkerhet som følger[48]:

> *Tiltak iverksatt for å sikre at informasjon ikke er tilgjengelig uten autorisasjon (konfidensialitet), at informasjon ikke uautorisert endres eller ødelegges (integritet), og at informasjon er tilstede og anvendelig for medarbeidere slik at pålagte oppgaver kan utføres (tilgjengelighet).*

Informasjonsikkerhet kan beskrives som sikkerhet for å bevare informasjon utifra de retningslinjer som er satt.

I dagens samfunn er det fokus på forholdet mellom tilgjengelighet og operabilitet. Det er viktig å kunne tilby brukerne av systemene den informasjonen de ønsker, dette kan man oppnå gjennom å gjøre informasjon tilgjengelig. Et eksempel er å lagre opplysninger på nett slik at de er tilgjengelig for søk og innsyn av enkeltpersoner. Tim Berners-Lee har definert tilgjengelighet på nett, og for nettsider[49],

> *The overall goal is to create Web content that is perceivable, operable and understandable by the broadest possible range of users and compatible with their wide range of assistive technologies, now and in the future.*

Oversatt vil det overordnede målet være å utvikle webinnhold som er lesbart, anvendelig og forståelig for et bredest mulig spekter av brukere og kompatibelt med teknologien i dag og fremtiden.
Dette vil øke tilgjengeligheten til informasjonen, men en slik løsning setter krav til operabilitet.

2.3 Folkeregisteret (DSF)

Det sentrale folkeregister (DSF) er et felles offentlig register for alle personer som er eller har vært bosatt eller skattet i Norge. Registeret ble i 1991 flyttet fra SSB til Skatteetaten og har siden det vært vedlikeholdt av Skatteetaten og danner grunnlaget for valg- og skatteberegning. DSF avviker for noen av reglene lovpålagt ved Personopplysningsloven, men har til gjengjeld egne regler og bestemmelser gjennom Folkeregisterloven. Folkeregisteret støttes opp av *Lov om folkeregistrering*[50] (Finansdepartementet, 1970), også kalt Folkeregisterloven. Denne tar for seg hvem og hva som skal registreres i DSF, i tillegg til bruk av registeret, meldeplikt og straff.

Både private og offentlige virksomheter benytter seg av informasjon fra registeret. Eksempelvis Skatte- og valgmyndighetene, offentlige virksomheter som NAV, UDI og Lånekassen for å nevne noen, og privte virksomheter som banker og forskringsselskap.

Videreformidling av personopplysninger fra DSF til offentlige virksomheter er avgjort gjennom § 14, første ledd i Folkeregisterloven.

[48] Datatilsynet, Informasjonssikkerhet, www.datatilsynet.no, http://www.datatilsynet.no/Sikkerhet-internkontroll/Informasjonssikkerhet/, ukjent, 16.11.2012

[49] W3C, Web Content Accessibility Guidelines (WCAG) 2.0, www.w3.org, http://www.w3.org/TR/2008/REC-WCAG20-20081211/, 11.12.2008, 05.02.2013

[50] Lovdata, LOV-1970-01-16 nr. 1: Lov om folkeregistrering (folkeregisterloven), www.lovdata.no, http://www.lovdata.no/all/nl-19700116-001.html, 01.01.2013 , 20.04.2013

§ 14. Uten hinder av taushetsplikten etter § 13, kan det i medhold av lov eller regler fastsatt av departementet, gis opplysninger fra folkeregisteret til offentlige myndigheter til bruk i deres virksomhet. For statistiske formål skal Statistisk sentralbyrå ha adgang til de registrerte opplysningene.

Skatteetaten lister opp informasjon som lagres i folkeregisteret[51];

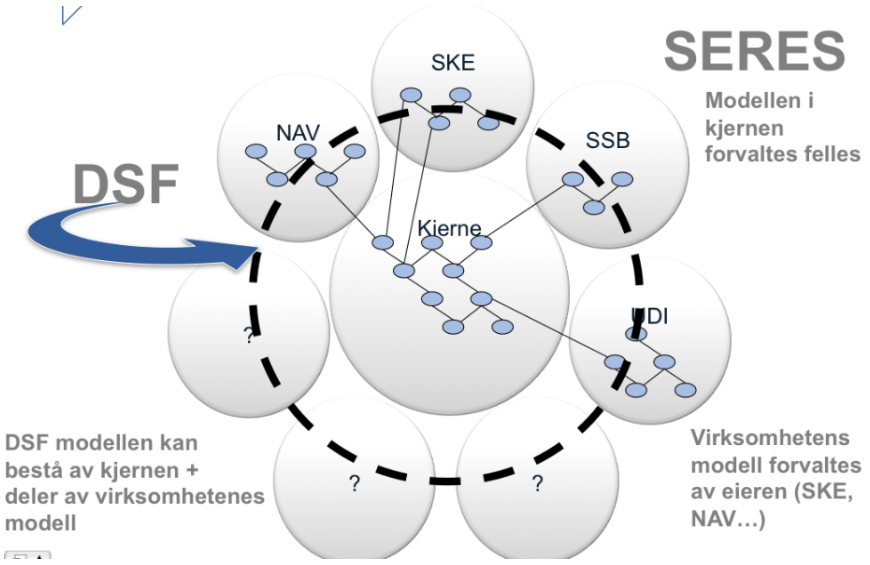
- *Fødsler, navnevalg, farskap og foreldreansvar*
- *Fødselsdatoendringer*
- *Flyttinger inn- og utland, postadresser og adressesperringer*
- *Sivilstandsendringer*
- *Dødsfall*
- *Navneendringer*
- *Statsborgerskap*
- *Vergemål*
- *Adopsjon*
- *Arbeids- og oppholdstillatelse*

Utifra listen vises det at omfattende personopplysninger lagres i registeret, noen av opplysningene som for eksempel familieforhold og familiehistorikk er konfidensielle personopplysninger.

2.3.1 Det nye Folkeregisteret

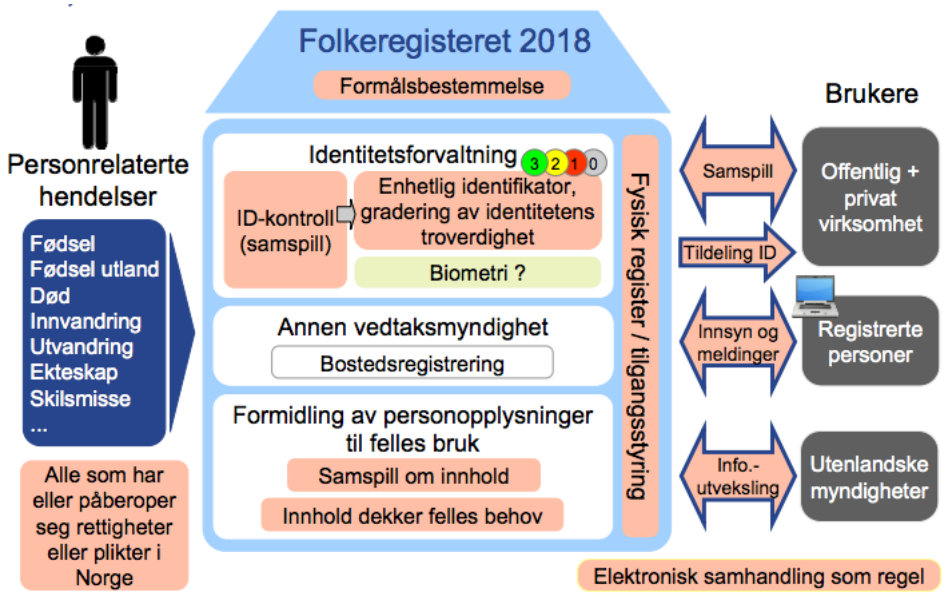
Skatteeaten foreslår en ny modell for benyttelse av folkeregisteret i offentlig sektor i forbindelse med innføringen av nytt personnummer i 2018. Her foreslås at DSF(Det sentrale folkeregister) kan bestå av kjernen, SERES (Semantikkregister for elektronisk samhandling), og deler av virksomhetens modell, som vist i Figur 2.2. Hvor virksomhetens modell forvaltes av eieren, mens modellen i kjernen forvaltes felles. Den tiltenkte modellen beskriver struktur i sammenheng med begreper eller informasjon, semantiske metadata og informasjonsmodeller. Metadata blir her beskrevet som informasjonsenhetes betydning, egenskaper og relasjon, samt eierskap, historikk og versjon. Det vil si en beskrivelse av informasjonen som ligger lagret i DSF.

[51] Skatteetaten, Folkeregister, www.skatteetaten.no,
https://www.skatteetaten.no/Alt-om/Folkeregistrering/, ukjent, 07.11.2012



Figur 2.2: Grafisk fremstilling av folkeregistetet som felleskomponent (Schürmann, 2012)

På eKommune-konferansen 24.-25. september 2012, presenterte Boris Schürmann fra Skattedirektoratet et foreløpig målbilde for Folkeregisteret 2018. Her vises hendelser rettet mot personer og personinformasjon mot ulike brukere. Brukerfokus er rettet mot samspill, tildeling av ID, informasjonsutveksling, i tillegg til innsyn og meldinger. Den mest omfattende og største endringen vil være enhetlig identifikator og gradering av identitetens troverdighet. Figuren viser at det er satt fokus på gjenbruk av persondata, med ivaretakelse av personvernet til den enkelte.



Figur 2.3: Målbilde av DSF 2018 (Schürmann, 2012)

2.4 Arkitektur

Det danske Digitaliseringsstyrelsen definerer arkitektur som en prosess som skal innføres og et resultat som skal implementeres[52]. Nærmere bestemt, fastsettelse av en klar ramme for oppbygningen av virksomhetenes systemer. En IKT-arkitektur er en skisse som viser hvordan en virksomhets systemer og infrastruktur er delt opp i mindre delsystemer og komponenter og hvordan disse henger sammen, samt hvilke prinsipper som legges til grunn for styring av disse over tid. Dette kapittelet vil gi en introduksjon til ulike arkitekturstandarder og virksomhetsarkitektur[53].

2.4.1 Infrastruktur

De fleste forbinder infrastruktur med den underliggende strukturen i samfunnet. En struktur som påvirker effektiviteten i samfunnet og omfatter alt fra veier til jernbaner, havner og flyplasser. En god infrastruktur kan måles i tilgjengelighet og kvalitet, begge grunnleggende faktorer for effektivitet[54]. I IT-sammenheng kan infrastuktur ses på som en felles betegnelse på komponentene i arkitekturen. Formålet med infrastrukturen er å knytte sammen elementene i en felles konstruksjon. Sikkerhet kan dermed ses som et viktig aspekt i IT-infrastrukturen.

Fokus på infrastruktur og kontinuerlig utvikling av denne i forhold til samfunnsutviklingen, er viktig for å kunne være endringsdyktig og kunne tilby det brukerne forventer.

2.4.2 Arkitekturstandarder

Arkitekturstandarder er viktig for å kunne oppnå samhandling og for å tilby felles grensesnitt mot og mellom systemene. Det er derfor utviklet standarder og retningslinjer for kvalitetsmodeller og informasjonsikkerhet.

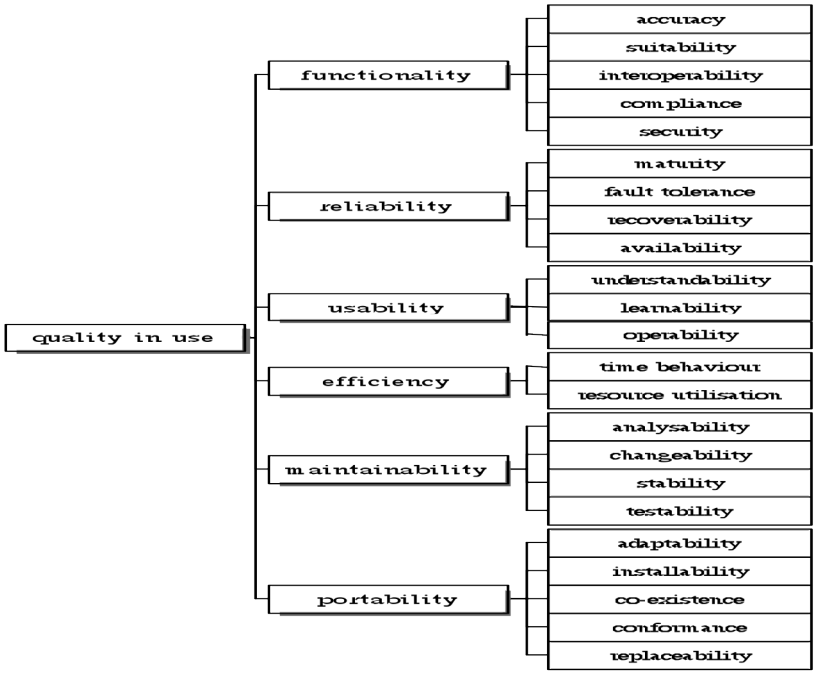
ISO 9126 - *Software Quality Model* og ISO 25000 - *Software Quality Requirements and Evaluation (SQuaRE)*

Det er utviklet standarder for produktkvalitet, ISO 9126 *Software Quality Model* (Oversatt: Programvarekvalitetsmodell). Standarden ser på seks kvalitetskarakteristikker for produktkvalitet, som vist i Figur 2.4. Disse er funksjonalitet (Functionality), pålitelighet (Reliability), brukervennlighet (Usability), effektivitet (Efficiency), vedlikeholdbarhet (Maintainability) og portabilitet (Portability). Funksjonalitet er den mest avgjørende faktoren for produktets kvalitet. Hovedbakgrunnen for utviklingen av standarden var å definere en felles forståelse for produktkvalitet og sette fokus på brukskvalitet.

[52] Digitaliseringsstyrelsen: Hvad er arkitektur?, www.digst.dk, http://www.digst.dk/Arkitektur-og-standarder/It-arkitektur/Om-arkitektur/Hvad-er-arkitektur, 30.04.2012, 03.02.2013

[53] Difi: Prosjektveiviseren, Begrep: IKT-Arkitektur:, www.prosjektveiviseren.no, http://www.prosjektveiviseren.no/begreper/ikt-arkitektur, ukjent, 12.11.2012

[54] SSB, Infrastruktur, www.ssb.no, http://www.ssb.no/emner/10/12/sa_transport/transport/infrastruktur.pdf, ukjent, 25.02.2013

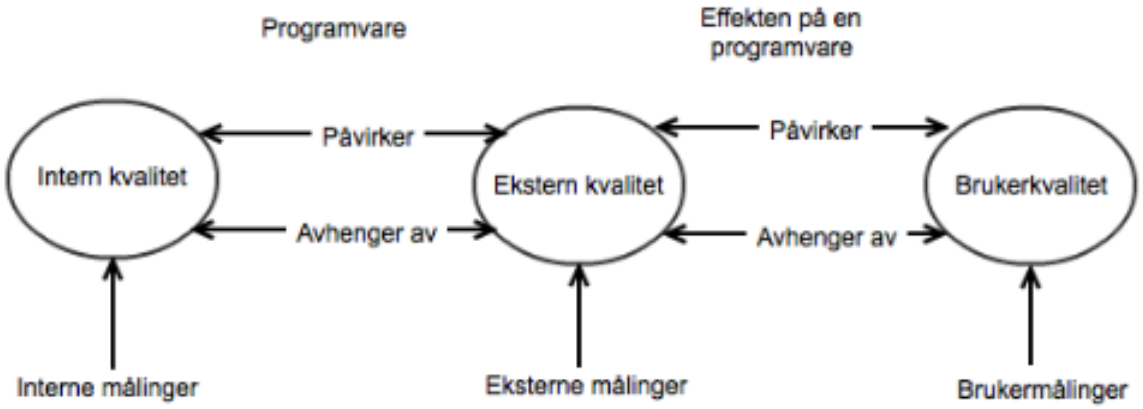


Figur 2.4: Ilustrasjon av ISO 9126 - Kvalitet i bruk

Standarden definerer kvalitet ved å benytte en faktor - kriterie - metrikkmåling (factor - criteria - metrics model). Det vil si at kvalitet er delt opp i faktorer, og hver faktor er igjen definert av et sett kriterier, som er definert av et sett beregninger. Det er kun mulig å gjøre antakelser på beregningsnivå. ISO 9126 opererer med tre beregningsnivå; intern, ekstern og brukerberegninger (Internal-, External- og User metrics) (Stålhane, 2010).

- Internal metrics (Interne målinger): Analyse av utviklingsprosessen for modell benyttet i forbindelse med estimering av ekstern kvalitet.
- External metrics (Eksterne målinger):Analyse av utviklingsprosesessen for modell benyttet i forbindelse med estimering av brukskvalitet.
- User metrics (Bruker målinger): Analyse av systemet for modell som benyttet i forbindelse med estimering av brukskvalitet.

Figur 2.5 viser de ulike beregningsnivåene for ISO 9126 og forholdet mellom dem.



Figur 2.5: Ilustrasjon av ISO 9126 (oversatt til norsk) - Tre nivå for beregning (Stålhane, 2012)

I 2005 ble ISO 9126 byttet ut med en utvidet utgave, ISO 25000 *Software Quality Requirements and Evaluation (SQuaRE)*[55]. I likhet med ISO 9126 evaluerer standarden programvarekvalitet og benytter interne og eksterne metrikker for knytte krav og evaluering. I tillegg til ISO 9126 sine seks kvalitetes karakteristikker for produktkvalitet inkluderer ISO 25000 også kompabilitet (Compatibility) og sikkerhet (Security).

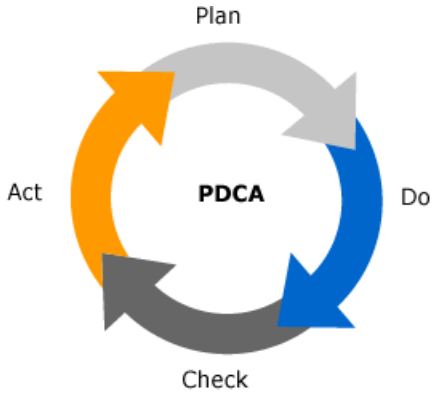
ISO/IEC 27000x - *Information Security Management Systems (ISMS) standards*

Standarden ISO/IEC 27000x, dekker informasjonsteknologi, sikkerhetsteknikker, informasjonssikkerhetssystemer og gir overblikk og ordforråd innenfor fagområdet informasjonssikkerhet. Målet med standarden er å gi informasjon til partene som er ansvarlige for gjennomføring av informasjonssikkerhet i en virksomhet[56]. Standarden legge vekt på risikostyring og gjør det klart at kun relevante retningslinjer må gjennomføres for å oppnå et tilfredstillende resultat.

Mange virksomheter velger å benytte ISO 27001 fordi den er egnet for å beskytte kritisk og sensitiv informasjon. I tillegg gir den helhetlig risiko-basert tilnærming for å sikre informasjon og overholdelse. Et annet viktig moment er at standarden kan demonstere troverdighet, tillit, trivsel og trygghet blandt kunder, partnere og utviklere.

ISO 27001 tilpasser seg prosessmodellen *PDCA, Plan-Do-Check-Act*, se Figur 2.6. PDCA benyttes som struktur i alle prosesser i ISMS. Prosessmodellen innebærer *Plan* (planlegge); etablere ISMS strukturen, *Do* (gjennomføre)*;* implementere og benytte strukturen, *Check* (kontrollere); oppfølging og gjennomgang av strukturen og *Act* (handle); oppdatere og forbedre strukturen.

[55]ISO, ISO/IEC 25000:2005, www.iso.org, http://www.iso.org/iso/catalogue_detail.htm?csnumber=35683, 17.12.2010, 28.04.2013
[56]CFN People, ISO/IEC 2700x, www.cfnpeople.com, http://www.cfnpeople.com/iso27000.html, ukjent, 13.12.2012



Figur 2.6: PDCA, Plan-Do-Check-Act prosessmodell

Et eksempel på bruk av PDCA kan hentes fra hverdagen; *Et verksted må reparere en bil for en kunde*[57].

- *Plan:* I planleggingsfasen må det tas hensyn til juridiske, regulatoriske og evt. forsikringsselskapets krav, samt bransjeforeningens og bedriftens retningslinjer og prosedyrer. Videre må det tas hensyn til produsentens instruksjoner, og gjøres vurderinger utifra betingelser, tidsaspekt og kontraktvariasjoner.
- *Do:* Gjennomføringsfasen inkulderer outsoursing av arbeid, innkjøp av deler, evt. spesialtjenester, planlegge utføring av arbeid ved å tilrettelegge for bruk av egnede verktøy og personer, i tillegg til journalføring.
- *Check:* Kontrollfasen innebærer kontroll og tester underveis i reperasjonsprosessen, i tillegg til ved ferdigstillelse. Dette innbærer også tilsyn/overvåkning av prosessen og tilbakemelding fra kunden.
- *Act:* Handlefasen inkluderer å løse eventuelle problemer.

2.4.3 Virksomhetsarkitektur

Difi definerer virksomhetsarkitektur i sin rapport *Overordnede IT-arkitekturprinsipper for offentlig sektor*[58].

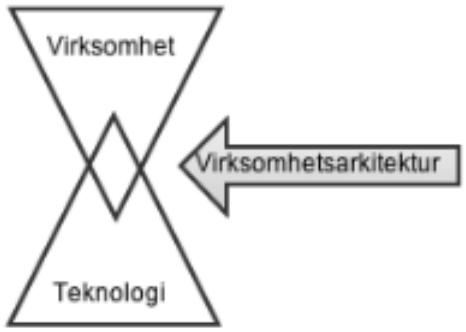
> *Virksomhetsarkitektur dreier seg om hvordan en virksomhet er organisert, hvordan arbeidsprosesser er satt sammen og hvordan IT-løsninger utnyttes. En virksomhetsarkitektur består av prinsipper, metoder og modeller som til sammen beskriver dette i en helhet.*

Virksomhetsarkitektur beskrives som sammenhengen mellom virksomheten og dens IT-teknologi. Målet med en overordnet virksomhetsarkitektur er å oppnå samhandling mellom nyutviklede enheter og prosesser som skal integreres i allerede eksisterende systemer. Dermed vil man oppnå en

[57] Qudos, Using the PDCA cycle in the real world, www.qudos-software.com, http://www.qudos-software.com/downloads/ApplyingPDCAcycle.pdf, ukjent, 06.04.2013

[58] Difi, Overordnede IT-arkitekturprinsipper for offentlig sektor, versjon 2.1, www.Difi.no, http://www.Difi.no/filearchive/arkitekturprinsipper-2.1.pdf,17.09.2012, 06.11.2012

helhetlig sammenheng i arkitekturen. Videre vil en gjennomtenkt virksomhetsarkitektur sette fokus på å tilpasse nye enheter til forretningsmessige behov. Figur 2.7 viser en overordnet modell av virksomhetsarkitektur, og forholdet mellom virksomhet og arkitektur.



Figur 2.7: Overordnet modell for virksomhetsarkitektur

Virksomhetsarkitektur kan føre til gevinst i den grad det fører til bedret datakvalitet, basert på økt effektivitet og produktivitet. Gjennom virksomhetsarkitektur tilrettelegges det for gjenbruk av eksisterende kompoenter og enheter i dagens løsninger og systemer[59]. Dette sikrer at investeringer og endringer støtter opp under foretningsbehov i virksomheten.

2.4.4 Distribuerte systemer

Et distribuert system er,

> *En samling av individuelle datamaskiner som opptrer ovenfor sine brukere som et enkelt sammenhengende system* (Oversatt fra engelsk, Tanenbaum, 2007).

Flere autonome datamaskiner kommuniserer gjennom et nettverk. Målet med distribuerte systemer er å koble tjenestetilbyder til tjenestesøker gjennom distribuert åpenhet, med fokus på skalerbarhet. Dette underbygges av egenskapene ved distribuerte systemer, nemlig åpenhet, parallelle prosesser, skalerbarhet, feiltoleranse og transperens[60].

Distribuerte systemer kan igjen deles i to, distribuerte operativsystemer og mellomvare (Mellomvarearkitektur forklares nedenfor).

[59] EDB ERGOGROUP FAGBLOGG: Landmark, Å lykkes med virksomhetsarkitektur, www.blogg.ergogroup.no, http://blogg.ergogroup.no/2010/01/21/a-lykkes-med-virksomhetsarkitektur/, 21.02.2010, 12.12.2012

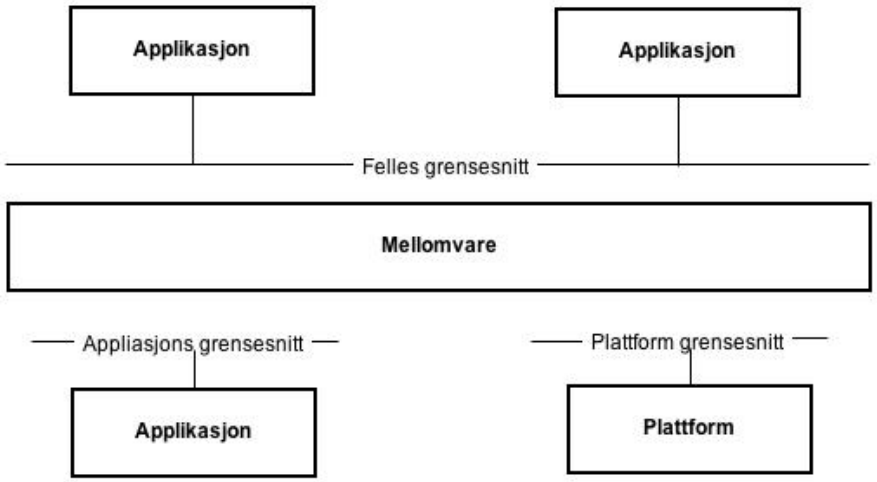
[60] Transparens betyr gjennomsiktighet og brukes i metodisk sammenheng om hvorvidt og hvordan detaljene i et studium beskrives. Stor grad av transparens betraktes som positivt for høy forskningsmessig kvalitet.

2.4.5 Mellomvare

Mellomvare defineres som,

> *En mellomvare er en generell tjeneste eller et programvarelag som befinner seg mellom en eller flere plattformer og overliggende applikasjoner.* (Oversatt fra engelsk, Bernstein, 1996).

Figur 2.8 illustrerer en overordnet mellomvarearkitektur. Figuren viser at mellomvaren ligger over plattformen (nettverket), men under appliasjonslaget (Bernstein, 1996). Mellomvaren kan beskrives som limet i en arkitektur med hetrogene komponenter eller systemer slik at disse kan samhandle på en standardisert måte uavheningig av implemnteringgsplattform.

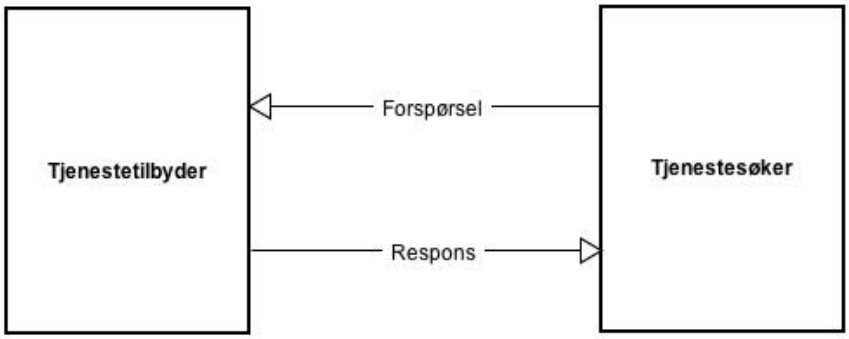


Figur 2.8: Illustrasjon av en arkitektur med mellomvare

2.4.6 Tjenesteorientert arkitektur (Service-oriented architecture)

Tjenesteorientert arkitektur eller Service-oriented architecture (SOA) blir definert som,

> *Tjensteorientert arkitektur er hovedsaklig en samling av tjenester som kommuniserer med hverandre. Kommunikasjonen kan involvere enkel sending av data eller flere tjenester som koordinerer en aktivitet* (Oversatt fra engelsk, Barry, 2002).



Figur 2.9: Illustrasjon av tjenesteorientert arkitektur

Ved hjelp av en tjenesteorientert arkitektur, kan man utvikle løst koblede systemer med et mellomlag i arkitekturen. Dermed skjermes tjenestesøkende fra endringene i tjenestene. En tjenesteorientert arkitektur oppfordrer og tilrettelegger for gjenbruk av komponenter, som medfører kostnadseffektivisering i forbindelse med integrering av systemer.

Figur 2.9 viser en enkel illustrasjon av tjenesteorientert arkitektur, hvor man har en tjenestesøker, som sender en forespørsel om en tjeneste fra tjenestetilbyder. Tjenestetilbyder sender en (tjeneste)respons til (tjeneste)søker.

Difi og standardiseringsrådet startet i 2010 arbeidet med å utvikle standarder for en felles tjenesteorientert arkitektur for offentlige virksomheter. Hovedfokus var å finne frem til felles standarder for utveksling av data mellom parter i offentlig sektor og mellom det offentlige og publikum basert på et tjenesteorientert perspektiv (Standardiseringsrådet, 2012).

SOA og Virksomhetsarkitektur

Virksomhetsarkitektur, som beskrevet i kapittel 2.4.3, er behovet for å se sammenheng mellom virksomhetens systemer og forretningsprosesser. SOA benyttes ofte i forbindelse med virksomhetsarkitektur da denne gjør skillet mellom teknologi og forretning mindre. Virksomhetsarkitekturen vil legge føringer på SOA. Den tjenesteorienterte arkitekturen vil videre gi føringer til virksomhetens integrasjonsbredde. Dermed er det viktig at virksomhetsarkitekturen og dens prinsipper bidrar til bedre utnyttelse av mulighetene innenfor SOA.

2.4.7 Skytjeneste-arkitektur

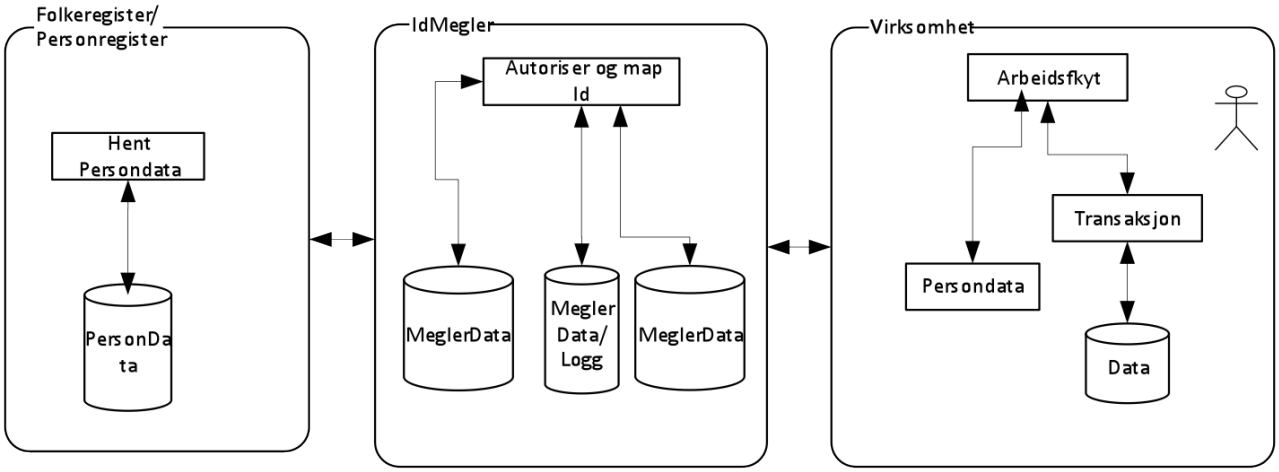
> *Hovedforskjellen mellom skytjeneste arkitektur og tradisjonell IT-arkitektur er at eier og bruker av sky-tjeneste arkitektur er separert i skyen* (Oversatt fra engelsk, Li, 2010).

Cloud Computing eller skytjenester er en IT-arkitektur som tillater kundene/brukerne/virksomhetene å benytte infrastrukturen, det vil si CPU, nettverk og lagringsmulighetene som ligger i skyen. Fordelene ved en slik arkitektur er reduksjon av kostnader, både i forbindelse med utvikling av egen

struktur, men også forvaltning av den. Skytjeneste er for mange bedrifter nytt og spennende, men også skummelt. Mange er usikker på sikkerheten og personvernet i skyen. Ingen bedrifter ønsker å miste kontrollen over sikkerheten i egne systemer. Dermed må det opprettes retningslinjer og delt sikkerhetsansvar mellom tjenestetilbyder, og bruker.

En av de største utfordringene i forbindelse med skytjenester, er sikkerhetsspørsmålet. Skytjenestetilbyderne skal sikre tjenesten de tilbyr og kan ikke overstige kundens myndighet.

2.5 IdMegler



Figur 2.10: Arkitektur for IdMegler(Sørensen, 2011)

IdMegler kan helt overordnet beskrives som et mellomvaresystem (se Kapittel 2.4.5), med roller. Dermed kan IdMegler opptre som et nøkkelregister for mapping av nøkler, og slik fremstå som en indeks mellom to systemer. Figur 1.2 viser tiltenkt arkitektur for IdMegler. Som vist på Figuren, kan den deles i tre, fra venstre et personopplysningsregister, IdMegler og en virksomhet.

IdMelger skal etableres for å gjøre identitetsmegling mellom en overordnet kilde for personopplysninger (for eksempel et personregister eller DSF) og saksbehandlingsdata relatert til personen. Hovedmålet med IdMegler er som bekrevet i bakgrunnen til masteroppgaven; *Koble sammen transaksjoner/saksbehandlingsdata med personopplysninger*. For å oppnå målet kreves noen forutsetninger. Disse er:

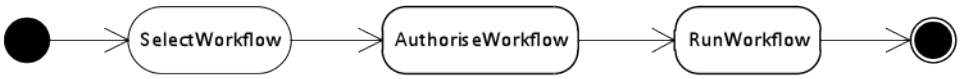
- *Personopplysninger ligger lagret fysisk adskilt fra saksbehandlingsdata.* Opprette et fysisk skille mellom statisk identifiserbare personopplysninger og saksbehandlingsdata, og annen dynamisk informasjon knyttet til person. Dette kan oppnås ved å skille ut personregistre på en slik måte at opplysningene i registrene ikke kan benyttes direkte for å finne annen type informasjon knyttet til person. I tillegg vil det være viktig å fjerne direkte identifiserende personkontekst på transaksjoner i databaser, og på den måte sikre at ved uautoriserte oppslag på transaksjoner så skal det ikke være mulig å koble disse til spesifikke personer. Basert på dette kan også alminnelig personopplysninger frikobles fra personidentifikasjon eller navn.
- *Transaksjonsdata benytter generert nøkkel fra IdMegler, og IdMegler inneholder kobling til personnøkkel.* For å sikre at virksomheter ikke skal kunne benytte gitt nøkkel til ikke-autorativ

aksess utenfor definert arbeidsflyt, kan nøkler relatert til person endres så snart arbeidsprosessen er ferdig. I tillegg vil det innføres en tidsbegrensning på nøklene for å sikre at man ikke "låser" opplysninger over tid.

- *Det er ikke mulig å benytte personnøkkel for å finne transaksjoner, eller transaksjonsnøkkel for å finne personer.* Tilgang til identifiserbar person og opplysninger knyttet til denne, må være veldefinert i modellerte og autoriserte arbeidsprosesser, med riktig autorisasjon på virksomhet, arbeidsprosess og saksbehandler. Dette muliggjør en kontroll over hvem eller hvilke aktører som benytter personopplysninger og til hvilke prosesser, ved benyttelse av logging. Videre vil adgang til data og personopplysninger være knyttet til spesifikke arbeidsprosesser som en del av ordinær tilgangsstyring i bedriften. Nøkler gjøres tilgjengelig på en slik måte at kontekst i arbeidsprosesser og autorisasjon styrer hvilke data som skal være tilgjengelig når. Basert på dette, vil virksomheters bruk av IdMegler forbedre ivaretakelsen av personvernslovgivingen.

2.5.1 Eksempel på bruk av IdMegler

Folkeregisteret (DSF) eller et overordnet personopplysningsregister inneholder basisinformasjon om personer, og kan tilgjengeliggjøre en identifikator (ikke meningsbærende fremmednøkkel) som kan benyttes av virksomhetsregister for å identifisere transaksjoner koblet til en spesifikk person.



Figur 2.11: Illustrert arbeidsflyt for IdMegler: Tilgangskontroll (Sørensen, 2011)

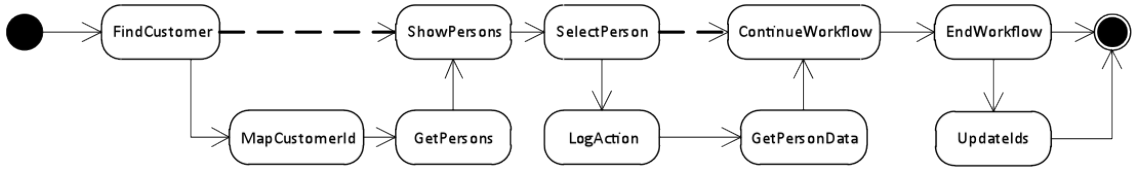
For å få koblet informasjon i et virksomhetsregister med DSF eller personopplysningsregisteret, må det defineres en arbeidsprosess med autorisasjon både på virksomhet, prosess og på person som utfører den for å tilgjengeliggjøre IdMegler for å koble sammen intern virksomhetsidentifikator med identifikator som kan benyttes til å finne relevante personopplysninger i DSF eller personopplysningsregisteret.
Figur 2.11 viser hvordan en autorativ person og prosess gir tilgang til IdMegler for mapping av id-er og koblinger av påkrevd personinformasjon til utføring av prosess i det normale systemet.

Figur 2.12 viser det normale systemet ved tilgangskontroll på prosess/arbeidsflyt.

Figur 2.12: Illustrert arbeidsflyt for IdMegler: Mapping (Sørensen, 2011)

IdMegler vil være ansvarlig for å tilgjengeliggjøre nøkler som benyttes i virksomhetens informasjonsregistre for å sikre at det er mulighet for en trygg sammenkobling med DSF eller personopplysningsregisteret. Alle transaksjoner relatert til person lagres dermed med nøkler tilgjengeliggjort gjennom

IdMegler og IdMegler benyttes for å sammenkoble opplysninger ved hjelp av nøkkelmegling mellom virksomhet og DSF, evt. personopplysningsregisteret.
Figur 2.13 viser hvordan logging av tilgang til bruker/virksomhet og prosess gjøres i IdMelger. Hvert oppslag i personregisteret logges med hvem, hva, når, og hvorfor oppslaget ble gjennomført. Logging blir skrevet til IdMegler for kvalitetsikring av arbeidsprosesser og innsyn i virksomhetens data om virksomhetens lagrede personopplysninger.



Figur 2.13: Illustrert arbeidsflyt for IdMegler: Mapping (Sørensen, 2011)

2.5.2 Bruk og utfordringer ved nøkkelgenerering, -endring og -megling

Nøkler er i hovedsak veldig store tall som brukes som innverdi i en krypteringsalgoritme. Nøkkellengden måles i bits, og i teorien vil en lang nøkkel være sikrere enn en kort nøkkel.

En av dagens største samfunnsutfordringer er gjenbruk av nøkler på tvers av systemer og bransjer. Personnummer er i stor grad misbrukt som nøkkel, siden personnummer er en personidentifikator som sjelden endres. Det finnes flere problemer knyttet til bruken av personnummer som nøkkel. Det er mange personer uten personnummer, og alle personnummer skal byttes ut innen 2018 ved innføringen av nytt personnummer. Ved bruk av IdMegler vil det være mulig å melde inn et nøkkelsett, og ved bruk av handshake (Rescorla, 2000) vil det tilbys nøkler basert på forespørsler og igjen opprettes koblinger mellom virksomhet og personopplysningsregister. I dette tilfellet får man tildelt nøkler, feks. URN (Uniform resource name), og den største fordelen vil være at ID ikke vil være meningsbærende (Schulzrinne, 2008). IdMegler kan også bidra til mapping av gamle personnummer med nye i forbindelse med utskifting av disse, for å unngå store endringer i allerede eksisterende systemer.

I mange tilfelle vil det være veldig sårbart å benytte en global ID på person. En løsning kan være å tilby en tjener, f.eks. IdMegler som mapper lokal ID med global ID internt, da vil det globale IDèn aldri bli offentliggjort.

2.5.3 Organisering av IdMegler

IdMegler som tjeneste kan etableres som et samarbeid mellom offentlige og private virksomheter. Det fulle potenstialet av tjeneste fra ett personvernssynspunkt, vil være å etablere en kobling mellom MinSide, IdMegler (som logger) og alle virksomheter som benytter IdMegler.

IdMegler som teknologi bør utvikles og forvaltes av et eget selskap eller organisasjon som etableres som et samarbeid mellom det offentlige, private virksomheter og representanter fra befolkningen.

2.6 Forskning på personvernsarkitektur

Det er gjennomført analyser, forskning og undersøkelser av dagens personvernsarkitekturløsninger

og fremtidstanker. Her trekkes det frem styrker og svakheter ved dagens løsninger (Solve, 1997), og konkrete mangler, som igjen viser behovet for en oppgradering for å kunne nå Personopplysningslovens krav og retningslinjer. Med bakgunn i dette, blir det foreslått mulige arkitekturer og infrastrukturer, basert på ulike teorier og teknologier som kan løse noen av dagens utfordringer.

RAIC (Redundant-Component Architectures)

En arkitektur som tar hensyn til personvern er *RAIC (Redundant-Component Architectures) (*Kobsa, 2003*). RAIC* består av en gruppe like eller identiske sammenkoblede komponenter. Eksterne applikasjoner kobler seg til *RAIC* og benytter den som en enkel enhet uten å vite om de underliggende komponentene i arkitekturen. Ved en forespørsel fra en applikasjon, benyttes en eller flere av disse komponentene for å dekke forespøselen. *RAIC* kan være statisk eller dynamisk og det er mulig å personalifisere komponentene, noe som medfører at arkitekturen kan benyttes til ulike formål.

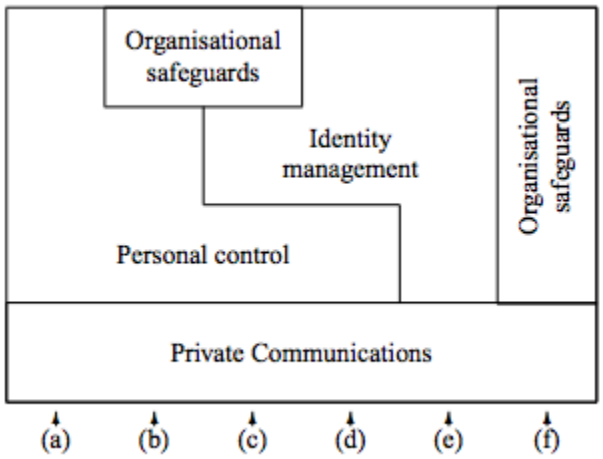
RAIC en fleksibel og dynamisk arkitektur for å personliggjøre metoder i forhold til lovgiving i applikasjoner, og kan ses på som en tilnæring til en mellomvare i en arkitektur.

LaPa (Layered Privacy Architecture)

LaPa (Layered Privacy Architecture) (Olivier, 2003) er en lagdelt arkitektur satt sammen av fire ulike lag for å oppnå et tilfredstillende sikkerhet- og personvernsnivå. Lagene som blir foreslått gjennom arkitekturen er;

- *Privat kommunikasjon (*Private communications*):* håndterer personvernsaspektet i forhold til kommunikasjon mellom ulike interessenter,
- *Organisatoriske beskyttelsestiltak* (Organisational safeguards)*:* refererer til bruk av teknologi for å sikre at organisasjoner overholder egne personvernsregler og preferanser til den enkelte,
- *Identitetsforvaltning (*Identity management*):* tar avgjørelser rundt privat kommunikasjon ved å vurdere årsakene til at noen foretrekker å jobbe anonymt eller under pseudonym,
- *Personlig kontroll* (Personal control)*:* refererer til bruk av teknologi for å sikre at den enkeltes personlige informasjon kun blir brukt i samsvar med den enkeltes personvern.

Figur 2.14 viser hvordan lagene kan kommunisere med hverandre. Det er mulig å kommunisere med et lag om gangen, *(a)-(c)*, eller en kombinasjon av de ulike lagene*(d)-(f)*. Hovedfordelen med arkitekturen er at man kan benytte ulike kombinasjoner av lagene for å oppnå ulike nivå av personvern.



Figur 2.14: Arkitektur for *Layered Privacy Architecture* (Olivier, 2003)

Egendefinerte personverns retningslinjer

Et alternativ til de lagdelte arkitekturene er å benytte seg av egendefinerte personverns retningslinjer (Langheinrich, 2002). Hovedideen bak arkitekturen er valg av sikkerhetsnivå, prinsipper og regler for systemene. Videre lages det retningslinjer for håndtering av brudd på disse, med påfølgende konsekvenser. De seks prinsippene som presenteres er;

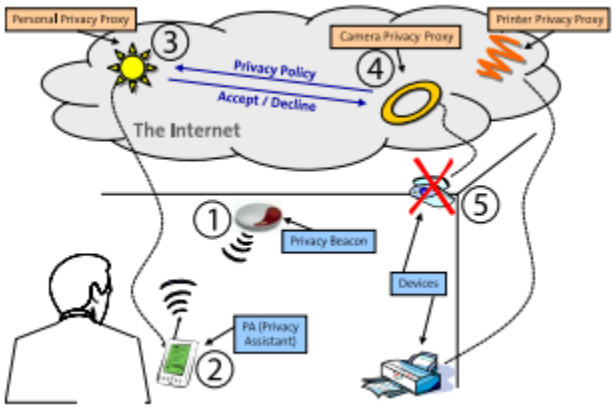
- *Varsel* (notice),
- *Valg og samtykke* (choice and consent),
- *Nærhet og lokalitet* (proximity and locality),
- *Anonymitet* (anonymity),
- *Pseudonymitet* (pseudonymity), og
- *Sikkerhet* (security).

Hvor *anonymitet*, *pseudonymitet* og *sikkerhet* benyttes som støtteverktøy i forhold til infrastruktur i applikasjoner, og ikke kan ses på som isolerte prinsipper. De tre hovedprinsippene som skal implementeres i systemet vil være i fokus gjennom utviklingen. Dette er;

- *Varsel:* deklarere praksis for samling av data og effektive måter å kommunisere disse til brukeren,
- *Valg og samtykke:* opprette sikkerhetsvalg for brukeren,
- *Nærhet og lokalitet:* støtte for tilgangsrestriksjoner i forhold til samlet data og behandling av forespørseler om å hente data fra en bestemt bruker,

- *Tilgang og ressurser:* brukerens måte å aksessere og logge data.

Figur 2.15 viser hvordan prinsippene benyttes i arkitekturen for systemet. Datainnsamlingen skjer i miljøet, 3, 4, som omringes av en sky. Her foretar også tjeneren kontroll av personvern opp mot brukerens preferanser, 5. Dersom disse ikke er like, vil forespørselen bli avvvist. Obligatoriske datasamlinger blir oppdaget i, 1, og detaljer rundt disse finnes i 2, som medfører at interessenter eller brukere holder relevante datasamlinger.



Figur 2.15: Arkitektur for *Privacy Management System* (Langheinrich, 2008)

2.6.1 Felles offentlig arkitektur eller infrastruktur

Difi, Direktorrat for forvaltning og IKT skriver i sin rapport, *Overordnede IT-arkitekturprinsipper for offentlig sektor* (Difi, 2012), om fordelene og ulempene ved innføring av en felles arkitektur eller infrastruktur for offentlig sektor. Rapporten undersøttes av Difi sin rapport, *Nasjonale fellekomponenter i offentlig sektor* (Difi, 2010), hvor det foreslås nasjonale fellekomponenter for offentlig sektor, samt tenkt bruk og nytte av dem. Hovedargumentene lagt frem i rapportene for innføring av en felles arkitektur, er økt kvalitet på data og informasjon gjennom brukerretting og økt kostnadseffektivitet. Gjennom felles retningslinjer skal det utvikles enkeltløsninger som realiseres i helhetlige digitale tjenester. For å forklare arkitekturprinsippene nærmere deles det opp i ulike kategorier. En av kategoriene er tjenesteorientering hvor hovedhensynet er funksjonalitet og ytelsesnivå, i tillegg til å tilrettelegge for gjenbruk. For å oppnå dette er det viktig å kunne samhandle med andre offentlige virksomheter, noe som sikres gjennom interoperabilitet og tilgjengelighet som innebærer tilrettelegging for gode og brukerrettede elektroniske løsninger. Andre viktige faktorer skalerbarhet, sikkerhet, fleksibilitet og åpenhet.

Norge er i dag rangert som nummer fire på området for IKT-infrastruktur i verden[61]. Gjennom videre utvikling med fokus på effektivitet og brukervennlighet for borgere, kan det skapes verdiøkning og flere arbeidsplasser. Økt informasjon og kvalitet rundt personvern vil føre til høyere grad

[61] Næringslivets hovedorganisasjon, IKT-INFRASTRUKTUR, www.nho.no, http://www.nho.no/files/IKT-infrastruktur.pdf, ukjent, 06.11.2012

av brukermedvirkning og en fordelaktig kvalitetspiral for brukerne. Lovverk og rettigheter rundt personvern er til liten nytte dersom borgerne ikke kjenner til forholdene.

> *I grove trekk kan det slås fast at det er meget krevende for en bevisst borger å finne informasjon om hvilke opplysninger en virksomhet behandler, hvordan opplysningene behandles eller hvilke rettigheter man har som registrert* (Datatilsynet, 2010).

2.6.2 Kommunikasjon ved bruk av personopplysninger

Behandling av bestemte personopplysninger til gitte forhold er lovpålagt og dermed uavhengig av borgernes samtykke, men det er imidlertid ingen lover som stopper virksomheter fra å kommunisere behandlingen. Dette gjelder også dersom innsamlede personopplysninger blir benyttet til andre formål enn forespurt eller blir formidlet til andre virksomheter. Personopplysningsloven § 20 regulerer nettopp dette. Ved å være åpen og kommunisere bruk, vil det bygges opp et tillitsforhold mellom virksomheten og enkeltpersonen, som igjen fører til økt kompetanse og kunnskap rundt personvern. Borgerne vil også få et helhetlig blikk over egne personopplysninger og hvordan disse benyttes.

2.6.3 Tilgangsstyrt bruk av registre

Gjennom analysen, *Fortell meg hva dere gjør!* (Datatilsynet, 2010), gjennomført av Datatilsynet, kommer det frem at private virksomheter er flinkere til å behandle og videreformidle personvern og personopplysninger enn offentlige. Begrunnelsen ligger i at for private virksomheter er det viktig å ivareta gode kunderelasjoner og opprettholde tilliten til kundene. Difi foreslår en løsning på bruk av felles komponenter gjennom rapporten, *Nasjonale fellekomponenter i offentlig sektor* (Difi, 2010). Her foreslås det opprettelse av grunndataregistre, eksempelvis Enhetsregisteret[62] og Folkeregisteret[63].

> *Behovet for grunndata på personinformasjonsområdet ivaretas i dag i utgangspunktet av Det sentrale folkeregister (folkeregisteret). Imidlertid vedlikeholder en del offentlige virksomheter også grunndata på personinformasjonsområdet i lokale registre* (Difi, 2010).

Dette fører til underbruk av folkeregisteret og igjen overbruk av lokale registre. Ved bruk av folkeregisteret direkte, vil det gi økt kvalitet og sikkerhetsmessige gevinster, og reduksjon av behovet for vedlikehold av lokale registre. Det er i dag store offentlige virksomheter som baserer seg på folkeregisteret sine opplysningene. Eksempelvis Nav, Skatteetaten og Lånekassen.

[62] Brønnøysundregistrene, Enhetsregisteret, www.brreg.no, http://www.brreg.no/registrene/enhet/, ukjent, 07.11.2012

[63] Skatteetaten, Folkeregister, www.skatteetaten.no, https://www.skatteetaten.no/Alt-om/Folkeregistrering/, ukjent, 07.11.2012

> *Elektronisk tilgang til folkeregisteret gis som hovedregel via de grensesnitt som tilbys av folkeregisterets distributør. Eksempler på grensesnitt er online oppslag, vask og uttrekk. Enkelte store statlige aktører, blant andre NAV, SSB og UDI, har inngått egne avtaler med Skattedirektoratet og vedlikeholder sine egne kopier av folkeregisteret basert på daglige endringstranser oversendt i batch direkte fra Skattedirektoratet* (Difi, 2010).

Offentlige virksomheter får ikke direkte tilgang til folkeregisteret, men lagrer egne lokale registre som oppdateres og sjekkes opp mot hoveddatabasen en gang om dagen. Gjennom rapporten argumenterer Difi for mangler og feil med informasjon som ligger lagret, samt svak kvalitet. I tillegg er det i dag en prisstruktur som fører til underbruk av folkeregisteret. Det argumenteres for at manglende informasjon i folkeregisteret fører til mindre bruk, av f.eks informasjon som elektronisk id, e-postadresse, telefonnummer, språk og målform. Enkelte virksomheter ønsker også informasjon om dataelementer som beskriver brukerens preferanser i forhold til kommunikasjon. Dette kan med fordel utformes universelt.

> *For at en sentral løsning skal fungere etter hensiktene er den avhengig av regelverket ikke er til hinder for utnyttelse av løsningen etter intensjonene* (Difi, 2010).

For at folkeregisteret skal tilfredstille ønskene og kravene som kommer frem av rapporten, må det gjennomføres en moderniseringsprosess. Dagens samfunn setter høye krav til effektivitet og samarbeid i ulike sektorer og globalt. Samfunnet står ovenfor en del konkrete problemstillinger som fornying av fødselsnummersystemet, udekkede brukerbehov, ID-tyveri, ulike prismodeller og et behov for teknisk modernisering (Schürmann, 2011). Videre kan vi se på faktorer knyttet til hvilke informasjon som skal være registrert, DSF sin rolle ved identifisering og autentisering, samt hvilken informasjon som skal videreformidles til samspillsaktører. Dette kan gjøres gjennom økt sikkerhet og personvern, bedre kvalitet, økt effektivitet og enklere bruk for borgere.

2.7 Dagens praksis

Dette kapittelet ser på dagens normer og forhold til personvern i eksisterende løsninger, i tillegg til Datatilsynets tendenser og utviklingstrekk.

2.7.1 Datatilsynet - Tendenser og Utviklingstrekk

Datatilsynets årsmelding fra 2011 ser på problemer relatert til personvern og lagring av store datamengder på nett (Årsmelding Datatilsynet, 2011). Årsmeldingen tar for seg hvor lite innsikt hver enkelt person har i personinformasjonen som ligger lagret i ulike registre og på nett. I tråd med den stadige økningen av personopplysninger på nett, vil også manglende kontroll over egen personinformasjon øke. En av grunnene for den økende mengden data på nett, er fremveksten av skytjenester og sosiale medier, i tillegg til muligheten for å behandle større mengder data. Dette gjør at enkeltpersoner mister kontroll og oversikt over opplysninger om seg selv, som igjen kan ses på som et brudd

på personvernet. Både det offentlige og private aktører er aktiv i forhold til å spre informasjon og registre på nett.

Årsmeldingen tar for seg;

> *Rettigheten til informasjon om, og innsyn i, behandling av egne personopplysninger er viktige personvernprinsipper. Et annet sentralt prinsipp er at innsamlede personopplysninger kun skal anvendes til klart uttrykte formål* (Årsmelding Datatilsynet, 2011).

Det kan trekkes direkte paralleller til Personopplysningsloven kapittel 3, § 18, første ledd, som igjen vil være med på å bedre hver enkelt persons kontroll over og innsyn i egne personopplysninger. Målet vil være å redusere bruk og tolkning av data utenfor opprinnelig kontekst. Det skal gis beskjed til personer dersom det samles inn personopplysninger og hvilket formål opplysningene skal benyttes til. Dette støtter igjen opp under reglene, implementering og innføring av *Datalagringsdirektivet, DLD.*

Årsmeldingen legger vekt på at nye virkemidler må tas i bruk og personvern må innføres i alle ledd. Ved at personvern er innebygget som et sentralt element i virksomheten, vil det være lettere for brukerne å utvikle tillit til systemene, og holde seg innenfor rammene til lovverket. Det vil også være kostnadsbesparende å tenke på personvern under utviklingen av nye systemer, men i første omgang argumenteres det for at personvern er et verdispørsmål for bedriftene.

Årsmeldingen argumenterer for at veien fremover er å; illustrere nytten av innebygget personvern, en konsekvensvurdering av personvernet, lovmessing forankring av personvernkonsekvenser og forskning på personvernfremmende teknologi. Som et resultat av dette konkluderer Datatilsynet med følgende utsagn:

> *Jo mer kontroll brukeren selv har over løsningen og hva den registrer, jo mer personvennlig er den* (Årsmelding Datatilsynet, 2011).

Datatilsynet årmelding fremhever kollektivbransjen, helse og innføring av omsorgsteknologi som eksempler og aktuelle for innføring av personvern i systemene.

2.7.2 Kollektivtransportbransjen - elektronisk bilitering

Det ble i desember 2011, presentert en felles norm for Kollektivtransportbransjen, utviklet i samarbeid mellom sentrale aktører i bransjen, Datatilsynet og Statens Vegvesen[64]. Ved å utvikle en felles løsning for alle aktørene i bransjen, vil det skape forutsigbarhet for tolkning av reglene og lovgivingen.

Normen tar for seg retningslinjer for behandling og utvikling av personvernslovlige systemer, samt etterlevelse og krav for oppfølging. Utviklingen av bransjenormen skulle avklare en rekke spørsmål i forhold til personvernlovgivingen. I tillegg hadde den en politisk bakgrunn, innføring av elektronisk

[64]Digi: Rossen, Sikrer anonyme reiser med e-billett, www.digi.no, http://www.digi.no/885278/sikrer-anonyme-reiser-med-e-billett, 15.12.2011, 04.09.2012

billitering for kollektivtransporten i Norge. Normens hovedmål er å sikre at personer kan reise anonymt med elektronisk billett. Alle skal kunne reise uten å oppgi hvem og hvor de er. Som uregistrert bruker skal du få like fordeler som registrerte personer, personer som har oppgitt opplysninger om seg selv. Samtidig har bransjen mulighet til å tilby tilleggsytelser mot personopplysninger.

For å ta hensyn til personvernslovgivingen, er det laget regler for oppbevaring og håndtering av personopplysninger, samt retningslinjer for utlevering av personopplysninger til Politi og myndigheter (Datatilsynet: Bransjenorm, 2011). Videre skal bransjenormen

> *skape forutsigbarhet for aktørene i tolkningen av regelverket, samt skape tillitvekkende og godt personvern for den reisende* (Datatilsynet: Bransjenorm, 2011).

Slik normen fremstår i dag, er det regler og retningslinjer for innføring av elektronisk billettering og personvernslovgiving. Dette gjelder allerede eksisterende systemer og utvikling av helt nye løsninger. Det er i dag ikke et felles system som benyttes, men det jobbes mot en felles fremtidig løsning. I forbindelse med utviklingen av en felles løsning, jobbes det også mot en felles database, *NOD, Nasjonal ordredatabase*. Databasen vil være et felles lagringsted for ordre, noe som i dag skjer offline, og i ulik grad hos de forskjellige aktørene. Samtidig som *NOD* ikke direkte lagrer personinformasjon, vil den indirekte inneholde koblinger til personinformasjon da den håndterer fjernadministrasjon og distrubusjon av reisekort [65].

Arkitektur for elektronisk billettsystem

Arkitekturen for utviklingen av elektroniske billettsystem er transaksjonsbasert og avtalen mellom reisende og transportør ligger lagret på det elektroniske reisekortet. Oppbygningen krever at reiseopplysninger fra hver enkelt transaksjon samles inn for å ivareta krav ved systemet. En transaksjon genereres ved at det elektroniske reisekortet vises frem for en kortleser. Det kan skje synkrone og asynkrone overføringer av data basert på tilgjengeligheten til systemet, online eller offline. For å identifisere en person eller bruker i systemet, benyttes kortnummer som identitet sammen med en transaksjonsteller. Kortnummeret brukes som verifikasjon i forbindelse med reiser, men også for å yte tilleggstjenester. Systemene samler bare inn data i forbindelser med reiser. (Det blir ikke lagret data i systemene dersom en bruker ønsker å sjekke gyldigheten på reisekortet.).

Figur 2.16 er en illustrasjon for avlesning og registrering av reisekort. Her hentet fra Ruter, i Oslo[66].

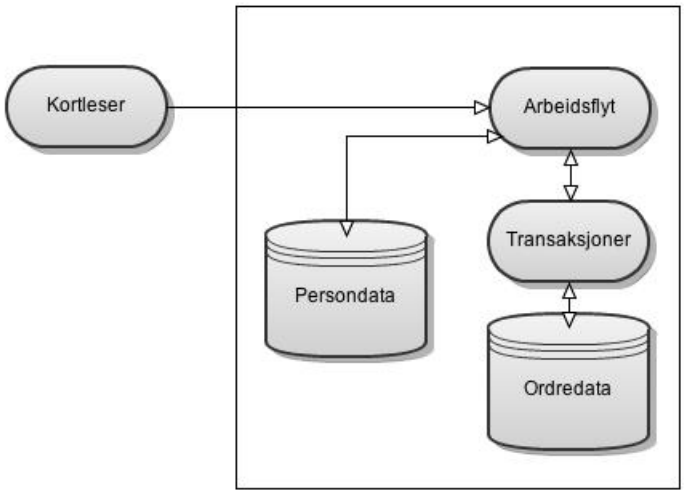
[65] Tekna: Hanssen, Innovasjonskonferansen for ITS og kollektivtransport: Nasjonal innretting for mobil billettering, www.tekna.no, http://www.tekna.no/ikbViewer/Content/828502/(17)%20Jorn%20Hanssen_IOAS%20AS.pdf, 19.10.2011, 04.09.2012

[66] Ruter, Aktivering - starte opp billetten, www.ruter.no, http://ruter.no/billetter/reisekortet/les_av/, 10.05.2012, 06.04.2013

Figur 2.16: Illustrasjon for mulig registrering og avlesning av reisekort.

Akitekturen tar opp problemstillinger knyttet til forskningsspørsmål 1, arkitektur som muliggjøre at man kan forholde seg anonym, men oppnå like fordeler som identifiserte brukere. Det er i dag et valg å ferdes anonymt i samfunnet og dermed må systemene basere seg på kundens samtykke, jf. Personopplysningsloven § 11, første ledd bokstav a, og § 8 første ledd. Normen tar for seg aktuelle problemstillinger for å ivareta kravet om anonymitet på internett. Anonymiteten kan svekkes ved logging og lagring av ip-adresser og cookies. Et annet aspekt er tilretteleging for anonymisering av personinformasjon slik at kunder som ønsker å være anonyme, ikke har mulighet til å oppgi personinformasjon. Retningslinjene er ikke direkte med på å forbedre anonymiseringen av personinformasjon, men gjør det mulig å forholde seg anonym ved bruk av systemet.

Arkitekturen skiller mellom transaksjoner og personopplysninger på et høyere nivå ved transaksjoner, se Figur 2.17. Bruker benytter sitt elektroniske reisekort. Ved kontakt med kortleseren starter transaksjonen. Det sendes en forespørsel til systemet og reisekortet sjekker kortnummer og avtale lagret i databasen. Forspørselen sendt til databasen bekreftes eller avbrytes og det sendes en tilbakemelding til bruker før transaksjonen avsluttes.



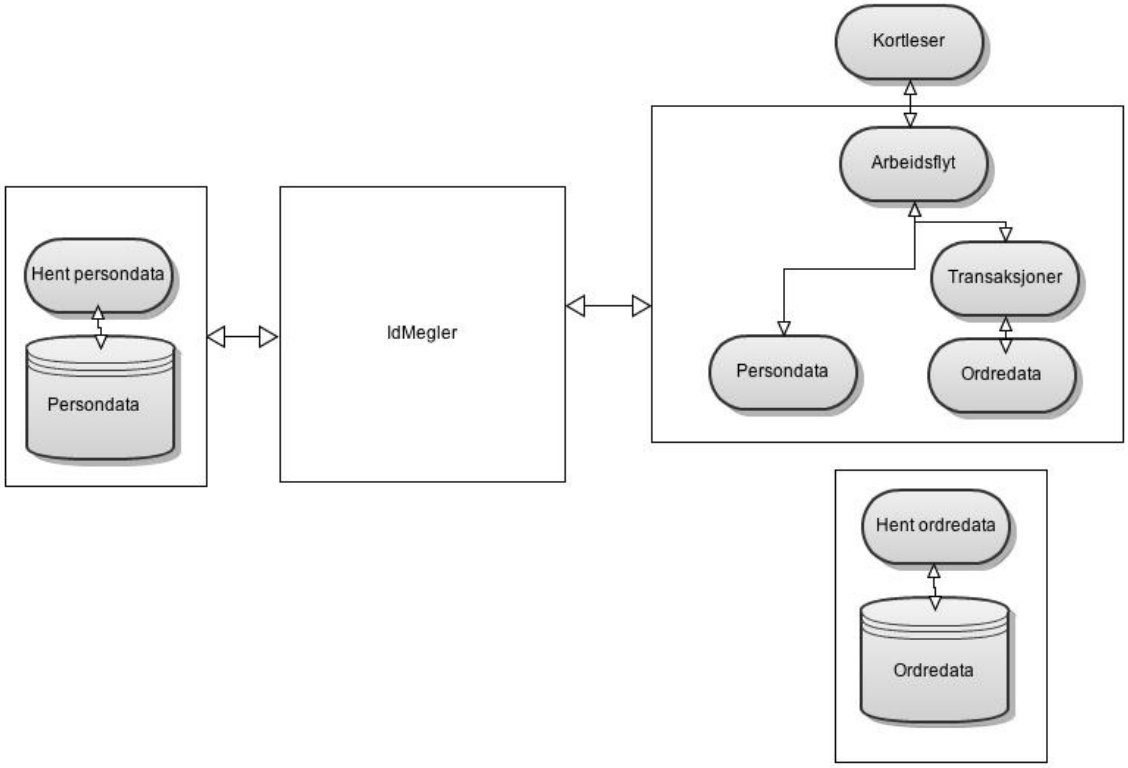
Figur 2.17: Illustrasjon av arkitektur for Kollektivtransportens bransjenorm

Bransjenormen har tatt hensyn til teknisk støtte og veiledning for få innsyn, hente ut, endre og slette lagret informasjon. Rettningslinjene vil være med å forenkle prosessene i forbindelse med

oppbevaring, håndtering og utlevering av informasjon. Innsynsrett er ikke styrt av brukers rolle. Virksomhetene har også plikt til å vedlikeholde og oppdatere informasjonen som ligger lagret og behandles i den lokale databasen. I utgangspunktet skal ikke personnummer benyttes, men i noen tilfeller, som skoleskyss, er dette nødvendig. Det er i hovedsak kortnummer som skal identifisere brukerne, men i noen tilfeller benyttes e-postadresse. Normen setter krav til sletting/anonymisering av data som skal gjøres innen 104 dager, eller etter endt kundeforhold.

2.8 Forslag til fremtidig løsning for kollektivtransportbransjen

En fremtidig løsning for kollektivtransportbransjen kan være et klarere skille mellom personopplysninger og saksbehandlingsdata. Som vist i Figur 2.18, vil det være mulig å implementere IdMegler for personopplysninger og *NOD* for saksbehandlingsdata/ordredata. Løsningen benytter IdMegler som mellomvare for å hente personinformasjon fra persondatabase, her kobles den direkte til ordredatabasen. Det finnes ulike muligheter, men ved å skille ordre- og persondata øker man sikkerheten i forhold til lagring av persondata, og muligheten for kontroll og oppfølging ved *DLD*.



Figur 2.18: Illustrasjon av mulig aktitektur fra kollektivtransportbransjen

IdMegler er en mellomvare og infrastruktur for integrasjon mellom mulige personregistre og virksomheter med eksterne applikasjoner og grensesnitt. Andre muligheter kan være lavnivå tjenester publisert direkte fra databasen, eller fra grensesnittet til applikasjonen, eller basere seg på samhandling og spesialutviklede komponenter (Difi: Tjenesteorientert arkitektur, 2010). Et viktig fokus

vil også være å ta for seg løsninger for mottakersiden, hvordan applikasjonen vil behandle personopplysningene som blir tilsendt fra personregisteret/databasen. Virksomhetene på mottakersiden har vanligvis allerede eksisterende systemer og arkitektur som det integreres mot, dermed vil det være ulike alternativer og løsninger for integrasjon med personregisteret/databasen. Et alternativ kan være direkte lagring i interne databaser, webtjenester eller spesialutviklede tjenester. Det er også mulig å benytte lokale databaser med manuell registrering av data, tilsvarende dagens løsning. Hovedfokuset i en godt implementert løsning vil være en helhet med sammenkobling av de ulike rollenes aktiviteter og et klart uavhengig skille mellom dem. Samtidig vil det være viktig å ta hensyn til interoperabilitet og teknologi, samt forretningsmessige betingelser for adgang til data (Difi: Tjenesteorientert arkitektur, 2010).

Difi foreslår to tekniske arkitekturløsninger i sin *Utredning av tjenesteorientert arkitektur i offentlig sektor* (Difi: Tjenesteorientert arkitektur, 2010). Det argumenteres for at et felles register kan muliggjøres ved en sentral tjeneste som IdMegler, eller ved kopiering av sentrale registre til en lokal database. Begge løsningene kan gi bedre ytelse og sikre tilgjengelighet avhengig av korttidsminnet og hvor komplekse de lokale databasene vil være. Ved å benytte kopiering til lokale databaser, er det flere hensyn som tas i forhold til oppdatering av lokale opplysninger. Dersom informasjonen ligger lagret i en fil, må filformatet tolkes, slik at det kan leses av databasen. Oppdateringene kan deretter overføres ved pull/push av hele databasen, enten endrings- eller hendelsesdrevet. Ved hendelsesdrevet arkitektur gis det beskjed til kilden dersom det er gjennomført oppdateringer. Hendelsesdrevet arkitektur kan løses gjennom transaksjoner mellom sentralisert arkitektur og lokale registre. Det er viktig å ta hensyn til systemet man skal integrere mot, samt dagens databasesystem og databaselogikk.

2.9 Sammendrag

- Personvern blir forbundet med interessen til å kontrollere formidlingen og bruk av opplysninger som angår en selv, når og til hvem, til hvilket formål og hvem opplysningene formidles til (Bing, 1991). Personvern er knyttet til praksis, i forhold til lovverket, arkitektur og dagens tekniske løsninger.
- Personopplysninger defineres gjennom Personopplysningslovens §2, som opplysninger og vurderinger som knyttes til en enkeltperson.
- Informasjonssikkerhet er en avveining i forhold til de fire faktorene *konfidensialitet, tilgjengelighet, integritet* og *kvalitet*.
- Folkeregisteret (DSF) er et felles offentlig register for alle personer som er eller har vært bosatt eller skattet til Norge.
- Ulike arkitekturløsninger og arkitekturstandarder kan ses i sammenheng med personvern og igjen ha gjensidig påvirkning på hverandre.
- IdMegler vil være en mellomvare mellom personopplysninger, eller tilgang til personopplysninger, arbeidsprosesser, saksbehandling og saksbehandlingsdata. Hovedoppgaven er å gi tilgang til koblinger mellom autoriserte klienter, samt logging av tilgang og bruk.
- Tidligere forskning på personvernsarkitektur inkluderer RAIC, LaPa og Egendefinterte personvernsrettningslinjer.

- Datatilsynet ser utfordringer relatert til personvern og lagring av store datamengder på nett knyttet til dagens praksis.
- Kollektivtransportbransjen her utviklet en felles løsning og norm for alle aktørene i bransjen. Målet med løsningen var å skape forutsigbarhet for tolkning av reglene og lovgivingen knyttet til personvern.

Del II

Forskning

3 Forskning/Metode

Under følger en oversikt over forskningstilnærming og metodevalg tatt i forbindelse med oppgaven. Kapittelet gir en innføring i metodene som er benyttet for oppgaven og hvordan disse er brukt for å besvare problemstillingen og forskningsspørsmålene.

3.1 Forskningstilnærming

Forskningstilnærming handler om å ta stilling til hvem og hva som skal undersøkes, og hvordan dette skal gjennomføres. Valg av metode betegner også valg av strategi for hvordan man ønsker å hente inn informasjon knyttet til det aktuelle problemet. Ved å benytte seg av forskningstilnærming, ønsker man å sikre pålitelig informasjon for å belyse problemstillingen innenfor gitte rammer (Ghauri, 2005). Forskningstilnærmingen kan deles i to tilnærminger, kvantitativ og kvalitativ metode.

Kvantitativ tilnærming

> *Kvantitativ tilnærming er strukturert og systematisert. Den går i bredden og tar sikte på å formidle forklaringer. Ved bruk av kvantitativ metode kan informasjon formes til målbare enheter. Dette muliggjør statistiske beregninger* (Dalland, 2007).

Kvantitativ tilnærming gir breddekunnskap, mulighet for å teste hypoteser og se på årsakssammenhenger. Gjennom bruk av kvantitative spørreundersøkelser, vil det samles data utifra en bestemt struktur som kan analyseres ved hjelp av statistiske metoder. Kvantitative undersøkelser gir konkret informasjon, men krever analyse og bearbeidelse av resultatene.

Kvalitativ metode

> *Kvalitativ metode har til hensikt å fange opp mening og opplevelse som ikke lar seg tallfeste eller måle. Den kvalitative tilnærming går i dybden og har som formål å få frem sammenheng og helhet. Den tar sikte på å formidle forståelse* (Dalland, 2007).

En kvalitativ metode vil være fordelaktig å benytte dersom man har lite eller uklar forkunnskap om tema som skal undersøkes. Gjennom metoden er målet å oppnå innsyn innenfor tema som vil gi kunnskap basert på erfaringer. Dette vil igjen gi et teoretisk gunnlag, med høy kvalitet innenfor et faglig perspektiv og en dypere informasjon rundt problemstillingen.

3.2 Metode

Et av målene ved oppgaven er å få innsikt i og forståelse rundt dagens arkitekturløsninger og mulighetene for endring. For å kunne oppnå endring, må adferd og holdninger blandt fremtidige brukere kartlegges. Det er også interessant å intervju forvalterne og utviklerene av fremtidige systemer.

Gjennom arbeidet for å kunne besvare problemstillingen, vil det benyttes ulike arbeidsmetoder. Metodene vil variere avhengig av forskningsspørsmålene som skal besvares. Personvernsarkitektur er som det ligger i begrepet, et tverrfaglig tema som kan knyttes til informatikk, jus, økonomi og politikk. For å oppnå et klart overblikk over dagens løsninger og fremtidens utfordringer knyttet til brukere og teknologi, er det benyttet både kvalitative og kvantitative metoder.

3.2.1 Litteraturstudie

Oates skriver i boken *Researching Information Systems and Computing* at hensikten med litteraturstudie er å samle og presentere bevis for å støtte påstanden om at du har utviklet ny kunnskap, at;

- Temaet er verdig,
- Studiet repeterer ikke tidligere gjennomført forskning og
- Du har skapt ny kunnskap som var ukjent fra før (Oates, 2006).

Hensikten med litteraturstudiet er å få innsikt i og forståelse rundt fagområdet, samt oversikt over tidligere forskning som er gjort innenfor temaet. Dette gjøres gjennom en orientering i hva som er kjent innenfor fagområdet og en systematisk gjennomgang av litteraturen rundt valgt tema. Litteraturstudiet gir ulike perspektiver på problemet og en konseptuell kontekst av problemstillingen.

Litteraturstudiet i denne oppgaven vil gi en innsikt i tidligere forskning, fremtidige planer, men også kanskje viktigst av alt, en innsikt i Norske lover og regler rundt personvern.

3.2.2 Spørreundersøkelse

> *Surveys refer to a method of data collection that utilizes questionnaires or interview techniques for recording the verbal behaviour of respondents* (Ghauri, 2005).

Oversatt til norsk forklarer Ghauri at undersøkelser viser til en metode for innsamling av data som benytter spørreskjemaer eller intervjuteknikker for å registrere verbal atferd ved respondentene.

I boken *Designing surveys : a guide to decisions and procedures,* beskrives tre viktige faktorer som må tas i betraktning når man benytter spørreundersøkelse som metode for datainnsamling, administrasjon og ressurser, utforming av spørreskjema og datakvalitet (Czaja, 1996). Videre utdypes begrepene,

- *Administrasjon og ressurser* refererer til økonomiske ressurser og tidsperspektiv i forhold til undersøkelsen.
- *Utforming av spørreskjema* handler i hovedsak om å finne de konkrete spørsmålene man ønsker å stille, samt hvor mange og hvilke type spørsmål man må stille for å gjennomføre studien.
- *Datakvalitet* handler om hvilken metode man tror appellerer mest til respondantene.

3.2.3 Dybdeintervju

> *I en intervjusamtale lytter intervjueren til hva folk selv forteller om sine opplevelser - lytter mens intervjupersonene med egne ord uttrykker sine oppfatninger og meninger, og lærer om deres tanker om arbeidssituasjon og familieliv, om deres drømmer og håp* (Kvale, 2001).

Et intervju er en forskningsmetode der intervjueren stiller intervjuobjektet spørsmål, som objekt besvarer. Intervjuer utføres vanligvis ansikt-til-ansikt, men kan også gjennomføres over telefon eller ved hjelp av andre hjelpemidler. Det er en veldig bredt benyttet forskningsmetode, men intervjuer er tidkrevende og setter store krav til forbedrelse, gjennomføring og etterarbeid. Dermed er det viktig å utvikle gode intervjuguider for intervjuene og gi intervjuobjektet en mulighet til å sette seg inn i tema og problemstilling før intervjuet (Robson, 2002).

Resultatene fra et intervju kan være vanskelig å strukturere og generalisere, dermed kreves det en form for profesjonalitet ved utforming av sammendraget og den tematiske oppsummeringen av intervjuet. Det kan også være fordelaktig å la intervjuobjektet lese gjennom og kommentere sammendraget for å rette opp i feil og misforståelser.

3.3 Valg av metode for forskningsspørsmålene

I kapittel 3.2, presenteres tre ulike forskningsmetoder, disse vil bli benyttet for å besvare forskningsspørsmålene. Kapittelet gir en innføring i hvilke forskningsmetoder som benyttes for å besvare de ulike forskningsspørsmålene.

- *FS1: Hvordan kan tjeneste-orientert arkitektur forbedre anonymiseringen av personopplysninger i forhold til Personopplysningsloven? og igjen være bidragsyter til å bekjempe identitetstyveri?*

Forskningsspørsmål 1 er todelt og tar for seg muligheten for økt personvern som et resultat av innføring av IdMegler-arkitekturen, samt muligheten for bekjempelse av identitetstyveri ved økt grad av innebygget personvern. Innebygget personvern handler i hovedtrekk om å ikke legge til rette for lovbrudd, enten med eller uten hensikt.

IdMelger-arkitekturen er en ny arkitektur, noe som gjør det vanskelig å finne relevante artikler og informasjon i litteraturstudie. Videre vil IdMegler arkitekturen kreve enn innføring og forklaring av prinsipper og retningslinjer for bruk, dette gjør at den ikke egner seg for spørreundersøkelser.

For å få innsikt i dagens arkitekturløsninger, mulighetene for innføring av IdMegler og økt personvern for den enkelte, vil det bli benyttet dybdeintervju. Det andre spørsmålet om ID-tyveri vil bli besvart gjennom litteraturstudie og spørreundersøkelser, med spørsmål rundt holdninger til identitetstyveri og tanker rundt økt fokus på innebygget personvern i fremtidige løsninger og systemer.

- *FS2: Hvilke teknologisk støtte/prosess har du som person i forhold til å hente ut/få innsyn i/slette personopplysninger om deg selv, lagret hos ulike virksomheter på nett?*

Lovverket setter regler og retningslinjer som virksomhetene må forholde seg til i forhold til innsyn og sletting av personopplysninger. Videre er det viktig å se på virksomhetens retningslinjer og

rutiner for å gjennomføre og følge opp disse. Forskningsspørsmålet belyser også problemstillinger rundt enkeltpersoners kunnskap og holdninger til personopplysninger, samt sletting og innsyn i dem. Dermed vil det være fordelaktig å benytte litteraturstudie, dybdeintervju og spørreundersøkelse for å kunne besvare forskningsspørsmålet tilfredstillende.

- *FS3: Er det mulig og hensiktstmessig å opprette en felles kilde til personopplysninger/et felles folkeregister for personopplysninger? Hvor stor del av opplysningene som lagres er statiske? og igjen hvor mange av dem er knyttet til bruk?*

Forskningsspørsmål 3 er et åpent spørsmål og appellerer til bruk av dybedeintervju for å avdekke fordeler og ulemper ved innføringen av et felles personopplysningsregister. Dybdeintervju kan også gi innsyn i dagens løsninger, og forholdet mellom statiske og dynamiske personopplysninger. I tillegg kan det være fordelaktig å se om lovverket tillater en slik løsning. Dette kan gjøre gjennom litteraturstudie.

- *FS4: Hvem eier informasjon som er lagret hos en virksomhet?*

Forskningsspørsmål 4 er et teoretisk spørsmål og egner seg i utgangspunktet best for en kombinasjon av litteraturstudie og dybdeintervju. Bagrunnen for dette er at eierskap til personopplysninger er lovpålagt i forbindelse med oppbevaring, lagring og sletting av personopplysninger. Videre er det viktig å finne hvordan virksomhetene forholder seg til lovgivingen og retningslinjene rundt dem. For å kunne besvare spørsmålet er det avgjørende å lese seg opp på og få en oversikt over lovverket, samt å få en innsikt i hvordan det gjøres/tolkes i praksis.

Basert på resonnementet er det valgt å benytte litteraturstudie, kvantitative spørreundersøkelser og kvalitative dybdeintervjuer for å kunne besvare forskningsspørsmålene tilfredstillende. Metodene vil gi innspill fra fremtidige brukere og aktører innenfor bransjen, samt forvalternes ønsker og behov.

3.4 Utvikling og utvalg

Delkapittelet omhandler utvikling og gjennomføring av spørreundersøkelsene og dybdeintervjuene. I tillegg presenteres det fem virksomhetene som det skal holdes dybeintervju hos.

3.4.1 Spørreundersøkelser

I løpet av arbeidet med oppgaven og besvarelsen av problemstillingen er det utviklet tre spørreundersøkelser;

- Spørreundersøkelse NOKIOS
- Spørreundersøkelse for studenter på NTNU
- Spørreundersøkelse for ansatte i IT-virksomheter

I første omgang ble det utviklet en spørreundersøkelse som ble delt ut på NOKIOS, Norsk konferanse for IKT i offentlig sektor. Dette var en 14 siders spørreundersøkelse bestående av 36 spørsmål om holdninger og erfaringer med tema rundt personvern og Personopplysningsloven. Spørreundersøkelsen var rettet direkte mot deltakerne på konferansen, aktører innenfor offentlig og private

virksomheter med høy akademisk bakgrunn. Bakgrunnen for spørreundersøkelsen var ønske om å få god innsikt i dagens løsninger og fremtidens alternativer.

Videre ble det utviklet to kortere og mer konkrete spørreundersøkelser. Dette var undersøkelser bestående av 20 spørsmål om respondentens kunnskaper og holdninger til personvern og dagens personvernslovgiving. Den ene av spørreundersøkelsene ble rettet mot studenter ved NTNU, den andre mot ansatte i norske IT-virksomheter.

De to siste spørreundersøkelsene ble utviklet på elektroniske skjema. Undersøkelsene startet med en kort introduksjon til tema og oppgaven, samt et par demografiske spørsmål om respondenten. Videre ble det stilt spørsmål om holdninger og kunnskap rundt personvern og Personopplysningsloven, samt bruk av respondantens personopplysninger og holdninger til offentlig mot private virksomheter ved lagring av personopplysninger. De fleste spørsmålene ble fremstilt som påstander gjennom oppgaven, og mulighet for å rangere svarene på en skala fra 1 til 6, hvor 1 tilsvarte, *i veldig liten grad*, mens 6, *i veldig stor grad*. Det var mulighet for å ikke besvare spørsmålene, ved å velge *Vet ikke*.

Spørreundersøkelsen delt ut på NOKIOS, finnes i Vedlegg B.1, mens den endelig utformingen av spørreundersøkelsen for studenter på NTNU finnes i Vedlegg B.2 og spørreundersøkelsen for ansatte i IT-virksomheter finnes i Vedlegg B.3.

3.4.2 Dybdeintervju

Litteraturstudie ga lite beskrivende og konkret informasjon om fremtidige personvernsfremmende infrastrukturer og dagens løsninger, ble det valgt ut konkrete offentlige virksomheter som kunne gi innspill rundt dette, gjennom dybdeintervju. Virksomhetene ble kontaktet gjennom bekjente i virksomhetene og via epost. Virksomhetene ble valgt utifra fag- og kompetanseområde, hovedsaklig virksomheter som behandler og lagrer store mengder personopplysninger. Basert på kriteriene ble Skatteetaten, Datatilsynet, Difi, PST og NAV kontaktet. PST hadde ikke mulighet til å delta på grunn av sikkerhetsmessige årsaker, mens NAV ikke kunne delta grunnet ressursmangel. Skatteetaten, Datatilsynet og Difi takket ja. I tillegg ble det valgt ut en offentlig bank, Sparebanken 1-gruppen og et oljeselskap, Statoil, for å få innspill fra privat sektor i andre bransjer. De deltakende virksomhetene er nærmere utdypet under.

Difi, Direktoratet for forvaltning og IKT

Difi (Direktoratet for forvaltning og IKT) bidrar til å utvikle og fornye offentlig sektor gjennom å tilby fellesløsninger og styrke samordning i det offentlige. Dette gjøres ved hjelp av spisskompetanse innen ledelse, utvikling av medarbeidere, IKT (Informasjons- og kom-munikasjonsteknologi), omstilling, organisering, kommunikasjon og offentlige innkjøp. Difi sitt mål er at den offentlige sektor skal ta i bruk deres løsninger, kunnskap, virkemidler og verktøy[67].

[67]Direktorat for fovaltning og IKT, Om Difi, www.difi.no, http://www.difi.no/om-difi, 01.08.2012, 22.01.2013

Difi har mange systemer og løsninger. Ved besvarelse i forbindelse med intervjuet, er det tatt utgangspunkt i ID-Porten, en felles påloggingsløsning og portal for telefonnummer og e-postadresser[68]. Det er mulig for ulike virksomheter å benytte seg av løsningen, og på den måten benytte seg av felles administrasjon av brukernavn og passord, samt brukerstøtte. Innlogging på ID-porten skjer ved høyeste sikkerhetsnivå, nivå 4 og brukerne kan benytte seg av elektronisk ID som MinID, BankID, Buypass og Commfides. Videre har ID-Porten høyt fokus på sikkerhet og tilgangsstyring, men behandler ikke data i høy grad.

Difi er i intervjuet representert ved Jon Berge Holden, gruppekoordinator for informasjonsikkerhetsgruppen til Difi i avdeling for digital forvaltning. Holden er utdannet jurist og har tidligere arbeidet 5 år i Skattedirektoratet med systemforvaltning, bl.a. av folkeregisteret.

Skatteetaten

Skatteetaten er underlagt Finansdepartementet, og har ansvaret for et oppdatert Folkeregister og at skatter og avgifter blir fastsatt og innbetalt på riktig måte. Videre arbeider Skatteetaten for å sikre finasieringen av velferdssamfunnet. Skatteetaten satser sterkt på utvikling og er ledende på innovative løsninger i offentlig sektor. Målet er å gjøre det enkelt å handle riktig[69].

I forbindelse med intervjuet tas det utgangspunkt i Skatteetatens nye løsninger, blandt dem Partsregisteret som er Skatteetatens nye felles løsning for å samle og tilgjengeliggjøre informasjon om Skatteetatens "parter", tilsvarende et felles kundesystem. I tillegg til Partsregisteret utvikles det ny tilgangskontroll, ATS (attributtbasert tilgangskontroll) som skal styre tilgangen til registeret.

Skatteetaten er i intervjuet representert ved Thomas Ringvår, konserntrainee med utdanning innenfor Forvaltningsinformatikk med en tverrfaglig master i jus og informatikk, Ole Alexander Moy, Prosjektleder for tekniske prosjekter og Torstein Talleraas, Arkitekt og ansvarlig for nye løsninger hos Skatteetaten.

Datatilsynet

Datatilsynet er både tilsyn og ombud. Gjennom tilsyn kontrollerer Datatilsynet at lover og forskrifter for behandling av personopplysninger blir fulgt og at feil og mangler blir rettet. Overordnet vil det si at arbeidet til Datatilsynet omhandler å medvirke til at den enkelte ikke blir krenket gjennom bruk av opplysninger som kan knyttes til enkeltpersoner. Gjennom rollen som ombud har Datatilsynet ansvar for å delta med rådgiving og informasjon til enkeltpersoner og publikum generelt[70].

Datatilsynet er representert ved Baar Larsen, konsulent hos Datatilsynet med erfaring innenfor privat og offentlig sektor.

[68] Difi, ID-Porten, www.difi.no, http://www.difi.no/digital-forvaltning/id-porten-minid, 12.12.12, 29.01.2013
[69] Skatteetaten, Vårt samfunnsoppdrag, www.skatteetaten.no, http://www.skatteetaten.no/no/Om-skatteetaten/Om-oss/Vart-samfunnsoppdrag/, 22.01.2013
[70] Datatilsynet, Datatilsynets oppgaver, www.datatilsynet.no, http://www.datatilsynet.no/Om-Datatilsynet/Oppgaver/, 27.11.2011, 22.01.2013

Sparebanken 1-Gruppen

SpareBank 1 Gruppen AS er et holdingselskap eid av SpareBank 1 Nord-Norge, SpareBank 1 SMN, SpareBank 1 SR-Bank, Sparebanken Hedmark, Samarbeidende Sparebanker AS og Landsorganisasjonen / fagforbund tilknyttet LO[71]. SpareBank 1 Gruppen har et administrativt ansvar for samarbeidsprosessene i SpareBank 1-alliansen, der teknologi, merkevare, kompetanse, felles prosesser / utnyttelse av beste praksis og innkjøp står sentralt. Alliansen driver også utviklingsarbeid gjennom tre kompetansesentre innenfor læring, betaling og kreditt. Sparebank 1-gruppen spenner fra forsikring, bank, forvaltning til eiendomsmegling og hovedmålsetningen er å være nær og dyktig.

Sparebanken 1-Gruppen er representert ved arkitekt Ole Petter Aasen.

Statoil

Statoil er et norskbasert olje- og gasselskap med betydelig internasjonal virksomhet. Selskapets formål er å drive undersøkelse etter og utvinning, transport, foredling og markedsføring av petroleum og avledede produkter samt annen virksomhet. Statoil har hovedkontor i Norge, om lag 21.000 ansatte over hele verden og er børsnotert i New York og Oslo[72].

Statoil er representert ved arkitekt Harald Wesenberg.

Gjennomføring av dybdeintervju

Det ble gjennomført personlige, semi-strukturerte intervju, som ga balanse mellom stablitet og fleksiblitet. Fleksibiliteten ga dybde og mulighet for oppfølgningspøsmål, stabliteten ga mulighet for analyse, sammenligning og mulighet for å trekke tråder mellom de ulike intervjuene.

Ved bruk av kvalitative intervjuer ønsker man å gå i dybden innenfor et tema. I den forbindelse ble intervjuobjektene informert om tema i forkant av intervjuet. Dette økte nivået på interjuvene, men også i forhold til andre relevante innspill til oppgaven.

3.5 Datainnsamling

Delkapittelet omhandler hvordan data ble samlet inn for spørreundersøkelsene og dybdeintervjuene, samt hvilke valgt som ble tatt i forbindelse med dette.

3.5.1 Spørreundersøkelser

Resultatene/Datainnsamlingen for de to siste spørreundersøkelsene ble innhentet i perioden 16.11.2012 - 17.01.2013 gjennom bruk av sosiale medier og NTNU sitt internnettverk.

[71] Sparebank 1, Om oss, www.sparebank1.no, http://pressesenter.sparebank1.no/om-sparebank1/, ukjent, 25.02.2013

[72] Statoil, Kort om Statoil, www.statoil.com, http://www.statoil.com/no/About/InBrief/Pages/default.aspx, 29.10.2009, 19.03.2012.

Datainnsamling ble for de to siste spørreundersøkelsene gjennomført ved hjelp av elektroniske spørreskjema utviklet i Google Spreedsheet[73]. Spørreskjemaene ble spredd/delt mot målgruppene ved hjelp av ulike sosiale medier som Facebook, Twitter, samt Innsida, NTNU sin internportal for studenter og ansatte. Dette ga en høy spredning til målgruppene i løpet av forholdsvis kort tid.

I oppgaven vil dermed NTNU-studentene og ansatte i IT-virksomhetene betraktes som (fremtidige) brukere.

Analyse

Analysen av den innsamlede informasjoen følger i kapittel 4. Kvantitative metoder kan analyseres ved hjelp av statisikk og svarene fra spørreundersøkelsene ble analysert ved bruk av programmet IBM SPSS versjon 20[74]. Programmet gir en god oversikt over innsamlet data, og tilbyr ulike behandlingsmuligheter. Ved analyse ble det i første omgang utviklet en beskrivende statistikk, som et grunnlag for en dypere forståelse av den videre analysen. Videre ble det benyttet faktor- og regresjonsanalyse.

3.5.2 Dybdeintervju

I forbindelse med dybdeintervjuene ble det utviklet intervjuguider til semistrukturerte intervjuer. Et semistrukturert intervju har en forhåndsutviklet intervjuguide; informanten følges opp gjennom bestemte temaer, ikke nødvendigvis fast rekkefølge og det er åpenhet for digresjon (Kvale, 2009). Bakgrunnen for valget av metoden var muligheten for innsikt i informantens perspektiver, erfaringer og tanker rundt de ulike tema. En slik intervjuform muliggjør også innhenting av fortolkninger og beskrivelser sett fra informantens hverdag.

Intervjuguiden ble delt i to hoveddeler, en del rettet direkte mot den respektive virksomheten og en generell del for alle virksomhetene. De generelle spørsmålene omhandlet kvalitetsikring og personvern i dagens og fremtidige løsninger. Delen direkte koblet til den respektive virksomheter, inneholdt spørsmål i forhold til virksomhetens arbeid og kompentanseområde.

Etter intervjuguidene var utformet, ble det foretatt et prøveintervju for å føle på situasjonen og erfare hvilke spørsmål som ga best uttelling i form av tilbakemelding. I forkant av dybdeintervjuene ble også intervjuobjektene informert om tema og problemstilling for intervjuene. Alle ble også informert om muligheten for å være anonym, samt muligheten for å trekke seg når som helst i løpet av intervjuet.

Intervjuene ble dokumentet ved hjelp av stikkordskriving, da mange ikke ønsket å uttrykke seg ved lydopptak. Det ble også utviklet korte sammendrag med sitater av de mest relevante temaene og spørsmålene som ble sendt til virksomhetene for godkjennelse for videre bruk i oppgaven.

[73] Google, Google Spreadsheets, www.google.com, https://developers.google.com/chart/interactive/docs/spreadsheets, ukjent, 29.10.2012
[74] IBM, SPSS software, www.ibm.com, http://www-01.ibm.com/software/analytics/spss/, ukjent, 29.10.2012

3.6 Måleproblematikk

Måleproblematikk benyttes for å se i hvilken grad datainnsamlingen har klart å måle det som var tiltenkt. For å kunne benytte de innsamlede dataene i en statistisk analyse og trekke troverdige konklusjoner, må det anslås reliabilitet og validitet. Reliabilitet vil si at målene er stabilie og robuste (konsistente) slik at resultatene ikke blir følsomme for små justeringer i instrumentet. Validitet omhandler måling av begreper og variabler i forbindelse med datainnsamlingen, at undersøkelsen har målet det den var tiltenkt å måle (Sannes, 2005).

3.6.1 Validitet og reliabilitet i spørreundersøkelse

Instrumentvalidering forsøker å kontrollere at spørreskjema representerer det fenomenet som studeres. Denne formen for validering handler om å kontrollere at spørreundersøkelsen fungerer i forhold til det man har tenkt å undersøke (Sannes, 2005). Instrumentvalidering i spørreskjema gjøres ofte ved bruk av faktoranalyse. Her kan man påvise mønstre i korrelasjonene mellom et sett av variabler med sikte på å undersøke om indikatorene måler en eller flere dimensjoner av et fenomen eller begrep. I tillegg kan man redusere datasettet ved å slå sammen variabler til et mindre antall faktorer basert på de sammenhengene man finner.

Instrumentvalidering vil bli gjort ved hjelp av faktoranalyse for de elektroniske spørreundersøkelsene, se Figur B.5, i Vedlegg B.2.2, *Analyse av spørreundersøkelse for studenter på NTNU* og Figur B.12, i Vedlegg B.3.2, *Analyse av spørreundersøkelse for ansatte i IT-virksomheter.*

Det settes krav og kriterier for bruk av faktoranalyse, blandt dem antall respondanter på undersøkelsen. For spørreundersøkelsen rettet mot studenter på NTNU vil 401 repsondenter være tilfredstillende. Spørreundersøkelsen rettet mot IT-Virksomheter har et mer beskjedent antall respondenter, 28, men vil benyttes for å støtte opp under den andre undersøkelsen.

For faktoranlayser forutsettes det at variablene er kontinuerlige, normalfordelte og med linære sammenhenger. En faktorladning viser grad av sammenheng mellom den enkelte indikatoren og faktoren som den inngår i. Faktorladningene varierer fra 0 (ingen sammenheng) og 1 (perfekt sammenheng).

Kriteriene som gjelder og er benyttet i oppgaven er:

- Kun faktorer med egenverdi større enn 1 blir beholdt i den roterte faktoranalysen.
- Faktorladningene må være større enn 0,5 for at et spørsmål skal tilhøre en faktor, evt. nest høyeste faktorladning for et spørsmål må være 0,3 eller lavere.
- Et spørsmål kan kun tilhøre en faktor.

For å få frem tydelige mønster mellom variablene vil *Direct Oblimin* (se begrepsordliste) benyttes. En slik rotasjon bidrar til å maksimere høye korrelasjoner mellom variablene og minimalisere lave korrelasjoner.

3.6.2 Validitet og reliabilitet i intervju

For å sikre validitet i et intervju er det viktig å stille spørsmål som gir svar på det som er ønskelig å måle. I hovedsak vil intervjuobjektene ha ulike interesser og holdninger rundt temaene og mange av disse er lov- og taushetsbelagt. Det er dermed viktig å lede intervjuobjektet på rett vei, men i tillegg stille spørsmål som åpner for diskusjon.

Det er viktig å sikre seg reliabilitet i forbindelse med intervju. Det vil at intervjuet ikke har målefeil påvirket av utenforliggende faktorer, som omgivelser eller misforståelser. For å oppnå reliabilitet har de skriftlige sammenfatting av intervjuene ble redigert og godkjent av intervjuobjektene i etterkant av intervjuene.

3.7 Sammendrag

- Forskningstilnærming handler om å ta stilling til hvem og hva som skal undersøkes, og hvordan det skal gjennomføres. Forskning kan deles i to kvantitativ og kvalitativ tilnærming.
- Gjennom oppgaven er det benyttet tre metoder, litteraturstudie, spørreundersøkelse og dybdeintervju.
- For å kunne besvare forskningsspørsmålene ble det utvikle tre ulike spørreundersøkelser og holdt dybdeintervju med fem ulike virksomheter, tre offentlige (Difi, Skatteetaten og Datatilsynet), og to privat virksomheter (Sparebanken 1-Gruppen og Statoil).

Del III

Analyse

4 Spørreundersøkelse

Gjennom kapittelet vil resultatene fra metodekapittelet bli behandlet og bearbeidet. Hensikten er å trekke konklusjoner rundt problemstillingen og forskningsspørmålene basert på undersøkelsene som er gjennomført. Kapittelet starter med statistisk analyse av spørreundersøkelsene, etterfulgt av oppsummering og analyse av dybdeintervjuene.

4.1 Spørreundersøkelse: NOKIOS

NOKIOS, Norsk Konferanse for IKT i offentlig sektor, er en konferanse lokalisert i Trondheim med aktører innenfor IKT i både privat og offentlig sektor. Det ble gjennom deltakelse på konferansen distribuert 120 spørreundersøkelser til deltakerne. En 14 siders spørreundersøkelse med 36 spørsmål om holdninger og erfaring med tema rundt personvern og Personopplysningsloven, se Vedlegg B.1, Spørreundersøkelse NOKIOS.

Spørreundersøkelsene ble skrevet ut og distibuert i papirform. Ved avslutningen av konferansen var det kun levert inn tre svar, og mange tilbakemeldinger rundt lengden og det tidkrevende arbeidet med å besvare undersøkelsen. I ettertid er det erfart at spørreundersøkelsen var for krevende, noe som resulterte i at det var vanskelig å få deltakerne til å besvare den. I tillegg ville besvarerne miste fokus underveis, noe som ville gitt dårlige svar mot slutten.

Det viste seg også at mange av spørsmålene kunne være for teknisk og irrrelevante for mange av deltakerne og hverdagen deres. Det ble også gitt tilbakemelding om at noen spørsmål var unødvendig da det er strenge retningslinjer og regler i offentlig sektor i forbindelse med personvern og informasjonssikkerhet.

Med bakgrunn i tilbakemeldingen ble det derfor laget to nye spørreundersøkelser, en rettet mot studenter på NTNU og en mot ansatte i IT-virksomheter.

4.2 Spørreundersøkelse: Studenter på NTNU

Nedenfor følger en tilnærmet kvantitativ analyse av *Spørreundersøkelse for studenter på NTNU*. Analysen starter med beskrivende statistikk etterfulgt av komponent- og overordnet analyse, før den avsluttes med en overordnet oppsummering.

Beskrivende statistikk

Beskrivende statistikk viser om de konstruerte variablene samsvarer med normalfordelingen og benyttes innledningsvis i analysen for å få en overordnet oversikt over resultatene fra spørreundersøkelsen.

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Q1.1	401	1	6	4.78	1.016	-.822	.122	.784	.243
Q1.2	401	1	7	3.73	1.140	.075	.122	-.514	.243
Q1.3	401	1	7	3.66	1.343	.140	.122	-.564	.243
Q1.4	401	1	7	2.61	1.295	.810	.122	.215	.243
Q2	401	1	7	1.95	.464	2.850	.122	35.719	.243
Q3.1	401	2	6	5.70	.599	-2.364	.122	6.722	.243
Q3.2	401	1	7	3.88	1.229	-.086	.122	-.436	.243
Q3.3	401	1	7	4.12	1.309	-.221	.122	-.619	.243
Q3.4	401	1	7	4.42	1.232	.135	.122	-.343	.243
Q3.5	401	1	7	2.31	1.545	1.671	.122	2.678	.243
Q4.1	401	1	7	3.91	1.422	-.323	.122	-.644	.243
Q4.2	401	1	7	3.68	1.362	-.012	.122	-.353	.243
Q4.3	401	1	7	3.79	1.179	-.259	.122	.086	.243
Q4.4	401	1	7	3.54	1.048	.198	.122	.892	.243
Q4.5	401	1	7	4.14	1.317	-.022	.122	-.144	.243
Valid N (listwise)	401								

Tabell 4.1: Beskrivende statistikk: Overordnet

Kolonnene minimum og maksimum i Tabell 4.1 viser laveste og høyeste verdi for svaralternativene for påstandene/spørsmålene i spørreundersøkelsen. For spørsmål/påstand 1.1 - 1.4 og 3.1 - 4.5 er laveste verdi 1.0, *veldig liten grad* og høyeste verdi 6.0, *veldig stor grad*. 7. 0 er benyttet i tilfeller hvor besvareren har svart, *vet ikke*. For spørsmål 2, betyr 1.0, *Ja*, 2.0, *Nei* og 3.0, *Vet ikke*.

Den beskrivende statistikken viser informasjon om "skewness" (skjevhet) og "kurtosis" (spisshet) for hver av variablene. Alle observasjoner innenfor hver variabel er plassert på en fem-punkts skala som former en kurve og normalfordeling vil gi en skjevhet på null. Negativ skjevhet viser at observasjonene er fordelt på høyre side, mens en positiv skjevhet viser at hovedvekten av fordelingen ligger til venstre for gjennomsnittet. Spisshet vil være null ved normalfordeling, spisshet over null gir en spissere kurve, mens spisshet lavere enn null resulterer i en flatere kurve (Juul, 2011).

Sannes (2005) setter toleransenivået på skjevhet og spisshet til 2,52 (1%-nivået), alternativt 1,96 (5%-nivået). Tabell 4.1 viser at det ikke er problemer med skjevhet i forbindelse med informasjonen hentet inn i spørreundersøkelsen, alle verdiene ligger under 2,52 (1 % nivået). I forhold til Kurtosis kan vi se et par spisser på kurven. På spørsmål 2 (Q2), *Har du bedt om innsyn i personopplysninger som er lagret om deg hos en virksomhet?,* og på påstand 3.1 (Q3.1) *Jeg forventer at personopplysninger om meg ikke skal bli benyttet til andre formål enn de jeg har gitt samtykke til.* Bakgrunnene for spissene er at mange av respondatene har svar likt på de gjeldene spørsmålene og bruk av disse resultatene kan påvirke den videre analysen. Verdien kan bli mindre enn virkeligheten representerer.

Standardavviket (Std. Deviation) bør helst ligge i nærheten av en eller høyere for å oppnå tilfredsstillende variasjon i dataene. Tabell 4.1 viser at et par variabler ligger under en, dette gjelder for spørsmål 2 (Q2) og spørsmål 3.1 (Q3.1).

Spørsmål 2 (Q2) har en Kurtosis på 35.719, og er et tre-svars-alternativ spørsmål. Av de 401 respondentene svarte 20 personer *Vet ikke* på spørsmålet, mens 84% av respondantene på spørreundersøkelsen har ikke bedt om innsyn i personopplysninger lagret hos en virksomhet. Påstand 3.1

(Q3.1) har en gjennomsnittsverdi på 5.70 og en Kurtosis på 6.722, dette er over 1%-nivået. Da begge spørsmålene også har et utilfredstillende standardavvik vil de bli utelatt fra den videre statistiske analysen.

For den videre analysen vil det bli tatt utgangspunkt i Tabell 4.2.

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Q1.1	401	1	6	4.78	1.016	-.822	.122	.784	.243
Q1.2	401	1	7	3.73	1.140	.075	.122	-.514	.243
Q1.3	401	1	7	3.66	1.343	.140	.122	-.564	.243
Q1.4	401	1	7	2.61	1.295	.810	.122	.215	.243
Q3.2	401	1	7	3.88	1.229	-.086	.122	-.436	.243
Q3.3	401	1	7	4.12	1.309	-.221	.122	-.619	.243
Q3.4	401	1	7	4.42	1.232	.135	.122	-.343	.243
Q3.5	401	1	7	2.31	1.545	1.671	.122	2.678	.243
Q4.1	401	1	7	3.91	1.422	-.323	.122	-.644	.243
Q4.2	401	1	7	3.68	1.362	-.012	.122	-.353	.243
Q4.3	401	1	7	3.79	1.179	-.259	.122	.086	.243
Q4.4	401	1	7	3.54	1.048	.198	.122	.892	.243
Q4.5	401	1	7	4.14	1.317	-.022	.122	-.144	.243
Valid N (listwise)	401								

Tabell 4.2: Beskrivende statistikk

Variabelkonstruksjon/Komponent Analyse

Prinsipial komponent analyse finnes i Vedlegg B.2.2, Analyse av spørreundersøkelse for studenter på NTNU, Figur B.6 og er basert på faktoranalyse og benytter følgende faktorer;

Faktor 1	BruddPersonvern (BP)	I hvilken grad man er redd for brudd på personvernet	(Q3.2, Q3.3, Q1.3, Q1.1)
Faktor 2	MisbrukPersonopplysninger (MP)	I hvilken grad man er redd for misbruk av personopplysninger	(Q4.2, Q4.1, Q4.3)
Faktor 3	KjennskapPersonvern (KP)	I hvilken grad man har kjennskap til personvern og Personopplysningsloven	(Q1.2, Q1.4)
Faktor 4	FrikoblingPersonidentitet	I hvilken grad personopplysninger skal frikobles fra personidentitet	(Q3.5, Q3.4, Q4.5)
Faktor 5	Snarveier	I hvilken grad personvern skal frikobles fra personidentitet	(Q4.4)

Tabell 4.3: Resultat av faktoranalyse

Basert på faktoranalysen og for å kontrollere fordelingsegenskapene til de nye variablene, er det viktig å foreta en ny beskrivende statistikk, se Figur B.7, i Vedlegg B.2.2, *Analyse av spørreundersøkelse for studenter på NTNU*, på variabelnivå. Denne viser fordelingsegenskapene på faktornivå. Etter

variabelreduksjonen kan vi se en jevnere skjevhet og kurtosis, alle er lavere enn 2,52, 1%-nivået.

Korrelasjonsanalyse

Correlations[c]

		Kjønn	Alder	Studieretning	Klassetrinn	BP	MP	KP
Kjønn	Pearson Correlation	1	.011	-.275**	.036	-.061	-.096	.081
	Sig. (2-tailed)		.819	.000	.466	.223	.055	.107
Alder	Pearson Correlation	.011	1	.133**	.609**	.079	-.021	.205**
	Sig. (2-tailed)	.819		.008	.000	.113	.672	.000
Studieretning	Pearson Correlation	-.275**	.133**	1	-.115*	.133**	.209**	.139**
	Sig. (2-tailed)	.000	.008		.022	.008	.000	.005
Klassetrinn	Pearson Correlation	.036	.609**	-.115*	1	-.011	-.063	.072
	Sig. (2-tailed)	.466	.000	.022		.830	.211	.153
BP	Pearson Correlation	-.061	.079	.133**	-.011	1	.036	.260**
	Sig. (2-tailed)	.223	.113	.008	.830		.467	.000
MP	Pearson Correlation	-.096	-.021	.209**	-.063	.036	1	-.069
	Sig. (2-tailed)	.055	.672	.000	.211	.467		.165
KP	Pearson Correlation	.081	.205**	.139**	.072	.260**	-.069	1
	Sig. (2-tailed)	.107	.000	.005	.153	.000	.165	

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

c. Listwise N=401

Tabell 4.4: Korrelasjonsmatrise

Tabell 4.4 viser korrelasjonsmatrisen for de konstruerte variablene og kontrollvariablene, kjønn, alder, studieretning og klassetrinn. Matrisen vil bli brukt som utgangspunkt for den videre analysen. POSITIV *Pearson korrelasjon* (Pearson Correlation, se begrepslisten) vil si at den ene variabelen gjennomgående svarer til en økning av den andre, mens NEGATIV korrelasjon vil gjennomgående svare til en reduksjon av den andre variabelen.

Overordnet analyse

Den overodnete analysen ser først på kontrollvariablene og de konstruerte variablene. Deretter tar den for seg spørreundersøkelsen tematisk.

Kjønn

Det finnes ingen utpregede kjønnsavhengige korrelasjoner med de sammensatte variablene, eller med forholdet til innsyn i personopplysninger lagret hos en virksomhet.

Alder

Alder kan ses som en avgjørende faktor for respondantens kjennskap til personvern, da alder korrolerer innenfor 0.01 nivået med den sammensatte variabelen KP. De yngste studentene i aldersgruppene under 18 år og 19-20 år korrolerer med negativ *Pearson korrolasjon* mot KP. De har lite kjennskap til personvern og Personopplysningsloven, i tillegg mener de at personvern er lite viktig for dem personlig. De eldste studentene i aldersgruppen over 31 år, korrolerer med positiv *Pearson korrolasjon* mot KP, det vil si at Personvern er viktig for dem personlig, og at de har kjennskap til Personopplysningsloven.

Studieretning

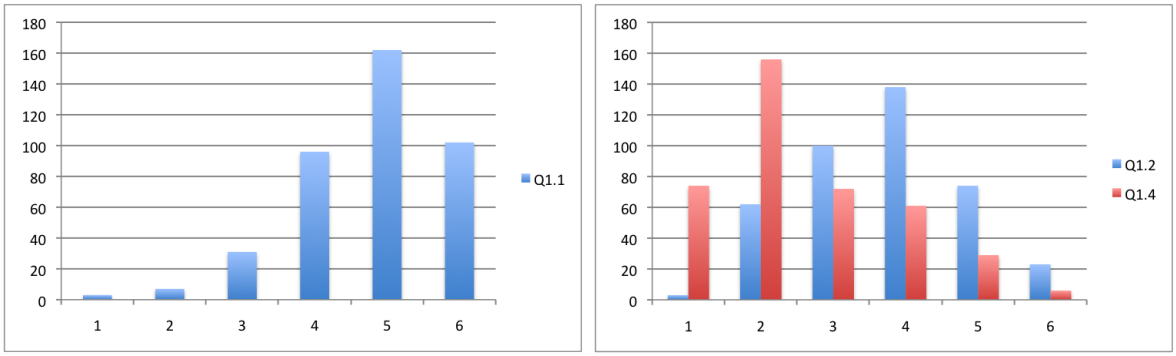
Basert på den statistiske analysen (ref. Korrelasjonsmatrisen, Tabell 4.4) ,viser det seg at studieretningen i høy grad avgjører respondantens holdninger og kjennskap til personvern. Studieretning korrolerer (Pearson Korrelasjon) innenfor 0.01 nivået med alle de sammensatte variablene, BP, MP og KP. Om vi trekker ut de ulike studieretningene korrolerer studie 1, *Sivilingeniør- og arkitektutdanning* innen 0.01 nivået med alle de sammensatte variablene, med negativ *Pearson korrolasjon*, mens studie 4, Annet (i hovedsak SVT-studenter) korrolerer med MP og KP, med positiv *Pearson korrolasjon*. Det vil si at studentene på de ulike studiene har ulike holdninger og kjennskap til personvern. Studie 2 og 3 korrolerer ikke med noen av de sammensatte variabelene.

Studenter på *Sivilingeniør- og arkitektutdanning* stoler mer på private virksomheter enn offentlige ved behandling og lagring av personopplysninger, mens studenter på andre studier stoler mer på offentlige virksomheter enn private ved behandling og lagring av personopplysninger. I tillegg har studenter på *Sivilingeniør- og arkitektutdanning* studiet høyere kjennskap til personvern enn de andre studieretningene.

Holdninger og kjennskap til personvern

Spørsmål 1 (Q1.1) i spørreundersøkelsen spør om repsondentens holdninger til personvern; *I hvor stor grad er personvern viktig for deg personlig?* Her har 25,4% av respondentene svart i veldig stor grad (6), mens hele 40, % har svart at personvern i stor grad (5) er viktig for dem personlig. Det vil si at 65,8% mener at personvern er viktig for dem personlig, se Figur 4.1 til venstre.

Figur 4.1 til høyre viser respondatenes kjennskap til personvern (blått) og Personopplysningsloven (rødt). Spørsmål 1.2 (Q1.2) omhandler respondentenes kjennskap til personvern. Her fordeler i stor grad svarene seg på svar alternativ 3, 24,9% og 4, 34,4%, slik at 59,3% har hverken stor eller liten kjennskap til personvern. Mens spørsmål 1.4 (Q1.4) spør om repsondentens kjennskap til Personopplysningsloven. 18,5% har i veldig liten grad (1) kjennskap til personopplysningsloven, mens hele 38,9% svarer de har liten grad av kjennskap til loven. Hele 57,4% av de 401 studentene ved NTNU har veldig liten, eller liten grad av kjennskap til Personopplyningsloven.



Figur 4.1: Kjennskap til personvern (venstre) og Personopplysningsloven (høyre)

Videre tar påstand 3.5 (Q3.5) for seg personlig brudd på Personopplysningsloven; *Jeg har tatt snarveier som bryter med Personopplysningsloven.* Her svarer 37,2% i veldig liten grad (1), mens

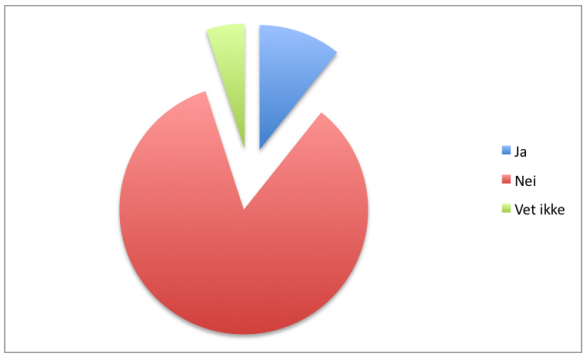
27,9% svarer i liten grad (2). Det vil si at 65,1% av respondentene svarer at de ikke har tatt snarveier som bryter med Personopplysningsloven. Her kan det diskuteres hvor vidt svarene er antakelser, da 54,7 % av respondatene har liten kjennskap til Personopplysningsloven.

KjennskapPersonvern (KP) og BruddPersonvern (BP)

Korrelasjonsmatrisen viser at de sammensatte variablene KP og BP korrolerer innenfor 0.01 nivået med positiv *Pearson korrelasjon*. De som har høy kjennskap til personvern er også i stor grad redd for et brudd på personvernet.

Innsyn i personopplysninger lagret hos en virksomhet

Sprøsmål 2 (Q2), *Har du bedt om innsyn i personopplysninger som er lagret om deg hos en virksomhet?* fikk som beskrevet tidligere, tilbakemelding som viste at 84% av respondentene ikke hadde bedt om innsyn i personopplysninger om seg selv lagret hos en virksomhet. Figur 4.2 viser fordelingen av respondantenes svar.



Figur 4.2: Fordeling Q2; Innsyn i personopplysninger lagret hos en virksomhet.

Respondentene som har bedt om innsyn er hovedsaklig i aldersgruppen 23-25 år og studerer et studie innenfor Sivilingeniør- og arkitektutdanning. De 16% som har bedt om innsyn har høy kjennskap til personvern, og er redd for å bli utsatt for brudd på personvernet. Disse respondentene har ikke et felles forhold til misbruk av personopplysninger og hvorvidt de stoler mer på private virksomheter enn offentlig når det kommer til lagring og behandling av personopplysninger.

De 84% som ikke hadde bedt om innsyn i lagrede personopplysninger har lav kunnskap om personvern, men er til gjengjeld redd for et brudd på personvernet.

De 20 personene som valgte å svare *Vet ikke* på spørsmålet om innsyn i personopplysninger har ikke en felles bestemt adferd eller holdninger til de sammensatt variablene. Dermed oppstår det ingen korrelasjon mellom dem.

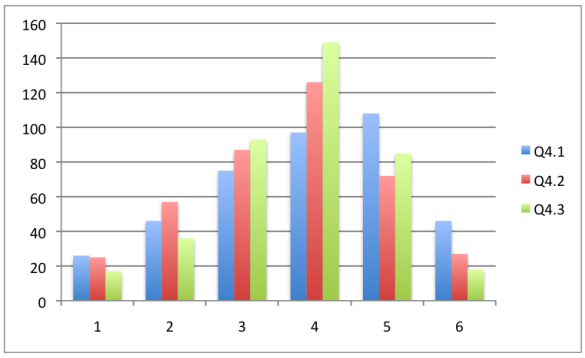
Bruk av personopplysninger

Som skrevet tidligere, ble påstand 3.1 (Q3.1), *Jeg forventer at personopplysninger om meg ikke skal bli benyttet til andre formål enn det jeg har gitt samtykke til,* tatt bort fra den videre statistiske analysen på grunn av et høyt antall like svar (høy Kurtosis). 76,3% (6) av respondentene har svart

at de ikke forventer at personopplysninger skal brukes til andre formål enn det er gitt samtykke til. Veldig mange av disse er også redd for et brudd på personvernet (BP).

Offentlig mot private virksomheter

Spørsmål 4.1 - 4.4 (Q4.1 - Q4.4) tar opp problemstillinger rundt lagring av personopplysninger i offentlige mot private virksomheter, Figur 4.3 viser fordelingen av respondentenes svar. Påstand 4.1 (Q4.1) tar for seg lagring av personopplysninger, *Jeg stoler mer på offentlige enn private virksomheter ved lagring av personopplysninger.* Her svarer 37,4% at de er veldig enig (6), eller enig (5) med påstanden. Det vil si at de stoler mer på offentlige virksomheter enn private virksomheter. Mens 18 % svarer at de er veldig uenig (1), eller uenig (2) med påstanden og stoler mer på private enn offentlige virksomheter. På påstand 4.2 og 4.3 (Q4.2 og Q4.3) om behandling av personopplysninger og økt fokus på sikkerhet rundt lagring av dem, svarer de fleste respondentene releativt nøytralt, verken for (4) eller mot (3). På påstand 4.2 har 53,1%, og påstand 4.3 har 60,4% svart (3), eller (4). Det vil si at respondantene ikke har så mye meninger rundt om virksomheten er privat eller offentlig.



Figur 4.3: Fordeling av offentlige mot private virksomheter, Q4.1 - Q4.3

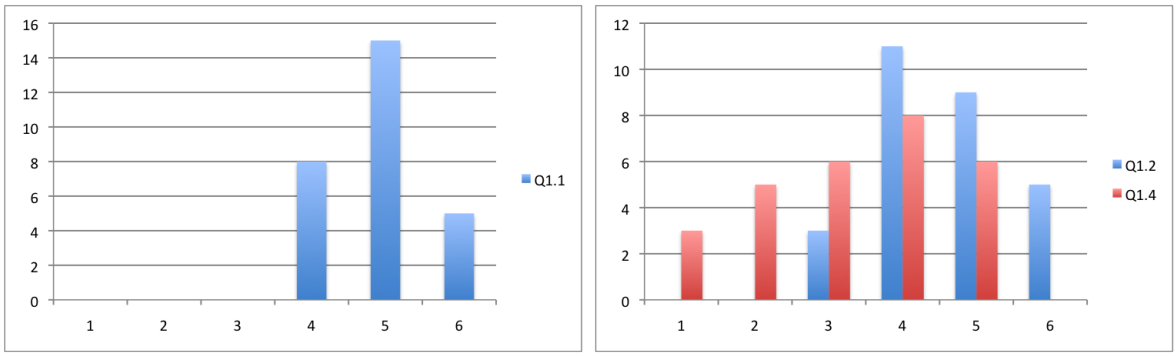
4.3 Spørreundersøkelse: IT-Virksomheter

Nedenfor følger en kort analyse av *Spørreundersøkelse for ansatte i IT-Virksomheter.* Spørreundersøkelsen benyttes for å støtte opp under *Spørreundersøkelsene for studenter på NTNU,* kapittel 4.2.

Spørreundersøkelsen er besvart av 28 personer, ansatt i ulike private og offentlige virksomheter, og tar for seg holdninger og kjennskap til personvern. Av de besvarende, jobber 87,6% i Privat sektor, 85,4% har høye utdannelse og 75% av resopondentene er menn.

Kjennskap og holdninger til personvern

Spørsmål 1.1 (Q1.1) spør om respondenten mener personvern er viktig for dem personlig. Her svarer alle respondentene på den øvre delen av skalaen, 4 - 6. Hvor den største andelen, 53,5% mener personvern er viktig i stor grad, se Figur 4.4 til venstre.



Figur 4.4: Kjennskap og holdninger til personvern (venstre) og Personopplysningsloven blandt ansatte i IT-Virksomheter (høyre)

Figur 4.4 til høyre viser respondentenes kjennskap til personvern (blått) og Personopplysningsloven (rødt). Her kan vi se at respondentene har relativt god kjennskap til personvern, men hvorvidt de har kjennskap til Personopplysningsloven sprer seg jevnt utover skalaen.

Innsyn i og misbruk av personopplysninger

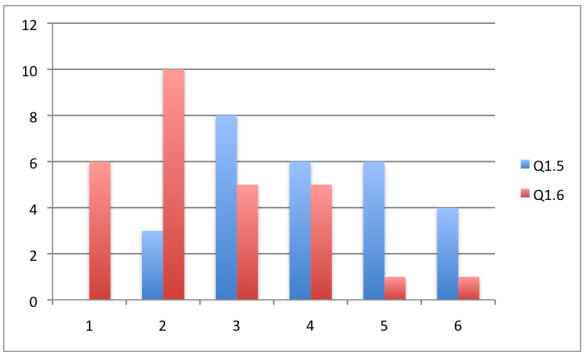
Spørsmål 1.7 (Q1.7), *Har du bedt om innsyn i personopplysninger som er lagret om deg hos en virksomhet?* viser at kun 14,3% av respondantene har bedt om innsyn i personopplysninger hos en virksomhet. Det vil si at 85,7% aldri har bedt om innsyn i personopplysninger lagret om dem selv, mens spørsmål 1.8 (Q1.8) tar for seg arbeidsplassens lagring av personopplsyninger; *Vet du hvilke personopplysninger din virksomhet har lagret om deg?* Her har hele 42,9% svar *Nei*, at de ikke vet hvilke personopplysninger arbeidsplassen lagrer.

Basert på faktorreduksjon og korrelasjonsmatrisen viser det seg at alder korrolerer innenfor 0.01 nivået med den sammensatte variabelene *Innsyn* og *misbrukPersonopplysninger*. Det vil si at alderen til respondenten er avgjørende for innsyn i og redselen for misbruk av personopplysninger. Videre viser det seg at kjønn korrolerer med 0.05 nivået og er avgjørende for i hvilken grad man er enig med påstand 2.4, (Q2.4), *Jeg mener det er en fordel at personinformasjon frikobles fra personidentitet.* Her mener menn i størst grad at en frikobling av personidentitet vil være fordelaktig. Alder korrolerer med påstand 2.3, (Q2.3), *Jeg er redd for at personopplysninger om meg skal bli benyttet uten mitt samtykke.* De eldste respondentene er de som i høyest grad er redd for misbruk av innsamlede personopplysninger.

Store personregistre

Spørreundersøkelsen tar for seg lagring av personopplysninger i offentlige mot private virksomheter. Spørsmål 1.5 (Q1.5) og spørsmål 1.6 (Q1.6) tar for seg store personregistre, henholdsvis, *I hvor stor grad er det foretrukket at det offentlige har store personregistre?* og *I hvor stor grad er det foretrukket at det private har store personregistre?* Figur 4.5 viser fordeling av svarene, og 74% av respondentene svarer på nedre del av skalaen, (1), (2), (3) og mener det er lite fordelaktig at det private har store personregistre. Videre viser Figuren at 14,3% av respondentene mener det i stor

grad (6) er fordelaktig at det offentlige har store personregistre. Dette viser at respondentene stoler mer på offentlige enn private registre og lagring av personopplysninger i dem.



Figur 4.5: Store personregistre i offentlige og private virsomheter

Offentlig mot private virksomheter

Videre blir respondanten presentert for påstand 3.1 (Q3.1), *Jeg stoler mer på offentlige enn private virksomheter ved lagring av personopplysninger* og påstand 3.2 (Q3.2) *Jeg mener at offentlige virksomheter har mer fokus på sikkerhet rundt personinformasjon enn private virksomheter.* Påstandene korrolerer, det vil si at de respondatene som stoler mer på offentlige enn private virksomheter ved lagring av personopplysninger, mener også at offentlige virksomheter har mer fokus på sikkerhet rundt personopplysninger enn private virksomheter. Bortsett fra dette, er svarene på de to påstandene jevnt fordelt utover skalaen.

4.4 Sammendrag

- Spørreundersøkelsene viser at det generelt er liten kjennskap til personvern og Personopplysningsloven. Det vil si at veldig mange ikke kjenner til rettighetene sine rundt lagring og innsyn i personopplysninger. Noe som igjen fører til personopplysninger kan bli misbrukt eller brukt til andre formål en tiltenkt. Mange har heller ikke oversikt over hvor og hvem som har tilgang til og lagrer personopplysninger om dem.

- Gjennom spørreundersøkelsen kan man se en kommende samfunnsendring etter innføring av store sosiale medier gjør at de yngste respondatene har et mye friere forhold til egne personopplysninger og spredning av disse. Det vil dermed være viktig å illustrere nytten av personvern og konsekvensene for den enkelte ved et brudd på dem. Videre kan det være viktig å gi brukerne en bedre oversikt over lagrede personopplysninger, noe som gjør det lettere å forholde seg til, endre og kontrollere.

5 Dybdeintervju

Gjennom dette kapittelet vil resultatene fra metodekapittelet bli behandlet og bearbeidet. Kapittelet starter med en tematisk oppsummering av dybdeintervjuet med NTNU, videre med de offentlige virksomhetene Difi, Datatilsynet og Skatteetaten, og til slutt med de private virksomhetene, Statoil og Sparebanken 1-Gruppen. Kapittelet avsluttes med dagsaktuelle scenarioer knyttet til de ulike undertema og en overordnet oppsummering av likheter og forskjeller knyttet til IdMegler og personvern.

5.1 Dybdeintervju: NTNU

Basert på restultatene funnet gjennom spørreundersøkelsen rettet mot studenter på NTNU ble det gjennomført et dybdeintervju med Jan Sverre Rønning, rådgiver i Seksjon for studieadministrative støttesystemer, Studieavdelingen. Her ble det stilt spørsmål rundt lagring og behandling av personopplysninger.

NTNU har i dag et felles student system (FS), eid og forvaltet av Studieavdelingen, for håndtering av studenter og studentopplysninger. Systemet henter informasjon og personopplysninger (kvalitetsikret mot DSF) om nye studenter fra samordna opptak. Systemet innholder også informasjon om oppmeldinger, semesterregistrering og rapporter i forhold til fremgang som sendes til blant annet Lånekassen.

FS innholder opplysninger om alle som har vært studenter på NTNU siden 1996/1997, med ca 20.000 aktive studenter per år. Det er 400 brukere med tilgang til systemet, alle disse administrativt ansatte, og det gjennomføres ikke logging og kontroll av innsyn i opplysninger lagret i systemet. Dette begrunnes ved at ingen av opplysningene i FS er sensitive, men noe av opplysningene kan likevell karakteriseres som konfidensielle.

Innsyn i personopplysninger

Personlig innsyn i personopplysninger lagret om en student vil gi informasjon om karakterhistorikk, oppstartssemester, semesterregistrering osv. Det vil også gi innsyn i eventuelle tilretteleggingger i forbindelse med eksamen og permisjoner. Søknader vedrørende tilretteleggingger i forbindelse med eksamen kan inneholde sensitive opplysninger da dette ofte er helserelatert. I slike tilfeller lagres kun resultatet av saksbehandlingsprosessen i FS, ikke saksbehandlingsgangen.

Oppslag på studenter i FS gjøres hovedsaklig ved hjelp av studentnummer eller personnummer.

Sletting av personopplysninger

Ingen informasjon i systemet slettes, det er kun statusen til hver enkelt student som endres basert på semesterregistrering. Det er offentlig informasjon og det må kunne sendes ut vitnemål på nytt. Det er kun de som har grunn til å logge inn i systemet som har tilgang, da administrativt.

Bruk av personopplysninger

Benyttes personopplysninger til andre formål enn det er gitt samtykke til?
Det har de siste årene vært saker angående tilgjengeliggjøring av studentlister inneholdende navn, adresse og oppnådd grad til rekrutteringsselskap. Noe som endte med saksgang og krav om at informasjonen måtte deles. NTNU ønsker i utgangspunktet ikke å dele informasjon med mindre man er lovpålagt, ref. Offentlighetsloven [75]. Noe informasjon kan også benyttes internt mot studenter og kartlegging av studenter.

Oppsummering

Basert på intervjuet viser det seg at NTNU lagrer lite sensitive personopplysninger i sine felles studentsystemer, men at det tilgjengjeld er lett å få tak i informasjonen gjennom innsyn og ved å ta kontakt med administrasjonen. Det er lett å misbruke systemet ved å hente ut informasjon uten å bli *registrert* da det ikke benytte logging og kontroll. Til tross for at personopplysningene i seg selv ikke er sensitive, kan en kobling av dem gi uheldige konsekvenser for den det gjelder. Videre gjennomføres det lite eller ingen sletting, noe som gjør at NTNU sitter på store mengder data om nåværende og (tidligere)studenter.

5.2 Dybdeintervju: Offentlige virksomheter

Difi, Skatteetaten og Datatilsynet er alle offentlige virksomheter. Difi er et statlig direktorat, Skatteetaten er underlagt Finansdepartementet og Datatilsynet er underlagt Fornyings-, Administrasjons-, og Kirkedepartementet. Virksomhetene har til dels ulike fagområder, men fellestrekket er at de lagrer, behandler eller sikrer personopplysninger, som er knyttet til personvernslovgivingen eller har en rolle som forvalter av lovverket knyttet til IT.

5.2.1 Tematisk sammenfatting av dybdeintervju

Personopplysninger

Personopplysninger er et begrep definert gjennom Personopplysningsloven og beskrives av Skatteetaten som grunnlagsdata.

Skatteetaten og Difi lagrer og behandler store mengder personopplysninger (over 3 millioner unike brukere), i henholdsvis Folkeregisteret/Partsregisteret og IdPorten. Personopplysningene håndteres/benyttes igjen i mange ulike systemer og til ulike formål. For eksempel samler Skatteetaten personopplysninger i forbindelse med Folkeregisteret, Skatt/likning og MVA-registre. Opplysningene og behandlingen av dem er lovregulert.

Difi benytter en database/et register for å lagre personopplysningene i ID-Porten, dvs formålsrettet, mens Skatteetaten benytter ulike kilder internt for lagring av personopplysninger, grunnet systemmessige krav.

[75] Lovdata, LOV 2006-05-19 nr 16: Lov om rett til innsyn i dokument i offentleg verksemd (offentleglova), www.lovdata.no, http://www.lovdata.no/all/hl-20060519-016.html, 16.12.2011, 06.04.2013.

Lagring av personopplysninger

Difi og Skatteetaten er store virksomheter med mange systemer og lagringsmuligheter, ulike registre, databaser og arkiver. Lagring av personopplysninger skjer hos Difi i digitale fagsystem og arkiv.

Skatteetaten lagrer personopplysninger direkte i fagsystemene. Dette skyldes at "Samfunnsoppdraget" til Skatteetaten er skatt-/likningsoppgjøret, det vil si, behandling av konfidensielle personopplysninger gjennom saksgang. Noe som fører til at det i tillegg til allerede lagrede personopplysninger vil oppstå nye personopplysninger gjennom saksbehandlingsprosesser i fagsystemene.

Tilgang til person- og saksbehandlingsopplysninger

Datatilsynet uttrykket at godt personvern innebærer varsling før bruk av lagrede personopplysninger. Gjerne med en begrunnelse på hvorfor og hva opplysningene skal brukes til, samt en forklaring på et evt. resultat i etterkant av saksbehandlingen. Eksempelvis kan det trekkes paralleller til varsling og gjennomføring av kredittsjekk på en person. Personen blir varslet i forkant av kredittsjekken, og informert om resultatet i ettertid.

Skatteetaten ser Datatilsynets ønske om en overordnet varslingsordning som problematisk. Talleraas utdyper dette med at; - *Noen interne forretnings/saksbehandlingsprosesser er i seg selv konfidensielle, ikke fordi de i seg selv inneholder personopplysninger, men fordi Skatteetaten ikke ønsker å informere om at de utføres. Et typisk eksempel er særskilte kontroller/analyser av enkelt-skattytere. Dersom kontrollen medfører funn, startes saksbehandling med kontakt med skatteyter.*

Innsyn i personopplysninger

Difi og Skatteetaten har retningslinjer for hvordan innsynsforespørsler blir behandlet. Hos Skatteetaten er dette en tidkrevende prosess fordi det skal samles informasjon fra Folkeregisteret og andre fagsystemer som skatt/avgift og likning. ID-Porten er et helt nytt system, noe som kun har ført til et fåtalls innsynsforespørsler. Basert på informasjonen som ligger lagret her er det ikke en tidkrevende prosess å få tilgjengeliggjort informasjon.

Talleraas uttrykte at det i forbindelse med innsynsforespørsler; - *Bør være begrunnede valg for å få innsyn i og hente ut informasjon. Samtidig er det ikke all informasjon og saksgang som det er mulig å utlevere informasjon om. I tillegg er det meste lovpålagt og lovregulert.*

Sletting av personopplysninger

Skatteetaten ble spurt om deres forhold til sletting av personopplysninger etter endt saksbehandling, samt i hvilken grad internkontroll ble benyttet for at personopplysningene slettes.

Ringvår uttrykker at sletting av opplysninger/personopplysninger i stor grad er lovpålagt; - *I forhold til hvor lenge opplysninger / personopplysninger skal lagres vil dette variere ut i fra opplysningenes art. For eksempel må regnskapsopplysninger oppbevares i ti år (red.adm ref. Regnskapsloven[76]) og*

[76]Lovdata, LOV-1998-07-17 nr 56: Lov om årsregnskap m.v. (regnskapsloven),

opplysninger av historisk verdi skal oppbevares i 20-30 år før det avleveres til riksarkivet (red.adm ref. Arkivloven[77]). I forhold til sletting av personopplysninger, er vi underlagt de krav som personopplysningsloven oppstiller (retningslinjer fra datatilsynet) så fremt vi ikke er noe annet er regulert i lov.

Et stort register - Folkeregisteret

Difi, Datatilsynet og Skatteetaten var alle enig om at et autorativt register for personopplysninger i fremtiden vil være fordelaktig (ref. Forskningsspørsmål 3). Hvorvidt Folkeregisteret kunne benyttes som autorativt register var det uenighet om.

Skatteetaten benytter Folkeregisteret som kilde til Partsregisteret, Skatteetatens nye felles løsning for å samle og tilgjengeliggjøre informasjon om Skatteetatens "parter". Innenfor Skatteetatens bruksområde, er ikke Folkregisteret alene tilfredstillende. Folkeregisteret skal holde informasjon om alle som har plikter og rettigheter i Norge, både norske og utenlandske statsborgere (personer identifisert ved D-NR og ikke fødselsnummer). Det er i tillegg mange utenlandske statsborgere i Norge over kortere eller lengre tid som ikke er registrert i Folkeregisteret, men som Skatteetaten har et forhold til.

Datatilsynet argumenterte for å sette fokus på kildene til personopplysninger, for å få et overordnet og tilfredstillende register. Om det autorative registeret var Folkeregisteret eller et annet register var ikke hovedfokus, men nærhet til lagrede personopplysninger ville øke personvernet og kvaliteten på innholdet i registeret. Videre vises det eksempelvis til flyttingen av Folkeregisteret fra SSB til Skatteetaten i 1991, for å oppnå nærhet til brukerne av de lagrede opplysningene.

Difi uttrykte også at nærhet til opplysningene lagret i registeret, basert på fagområder vil være fordelaktig. Virksomhetene med størst kunnskap innenfor et fagområde burde behandle og vedlikeholde opplysninger innenfor et bestemt tema.

Difi og Datatilsynet så utfordringer knyttet til et stort personregister, og mange brukere av dette. Det vil settes stor krav til oppetid, tilgangsstyring og behandling av forespørsler osv i et stort register. Larsen i Datatilsynet uttrykker store problemer med tilgangsstyring i store registre; - *Helt konseptuelt: tilgangsstyring i store registre er vanskelig, om nesten ikke umulig!* Videre fortsetter han: *I mange systemer må man pålegge logging for å avdekke stygge ting. Dette er overvåkning av de ansatte. I mange tilfeller vil det være bedre å opprette styringskontroll, og slipp å ettersjekke logger.*

Alle virksomhetene oppsummer til slutt med at det alltid vil være behov for et register i fremtiden uavhengig om det er på fysisk eller logisk nivå. Om det er overordnet, lokalt eller Folkereigsteret er ikke så lett å si.

---

www.lovdata.no, http://www.lovdata.no/all/nl-19980717-056.html, 17.07.1998 , 29.01.2013

[77] Lovdata, LOV-1992-12-04 nr. 126: Lov om arkiv (arkivlova),
www.lovdata.no, http://www.lovdata.no/all/nl-19921204-126.html, 12.04.1992 , 29.01.2013

Tilgangskontroll/Tilgangsstyring

Datatilsynet uttrykre at lekking av opplysninger til feile personer og på feil grunnlag er vanskelig om ikke umulig å rette opp. Dermed er det viktig å fokusere på å begrense tilgang til informasjon og ikke være avhengig av kontroll og overvåkning i ettertid.

Alle virksomhetene uttrykte enighet om at situasjonsbasert- (Difi), attributtbasert- (Skatteetaten) eller beslutningsstyrt- (Datatilsynet) tilgangskontoll er avgjørende for økt kvalitet på lagrede personopplysninger og høyere personvern for den enkelte. Dermed vil det være viktig å fokusere på tilgangskontroll som er nært knyttet til sakbehandling og saksgang. Tilgangskontrollen forteller hva og hvorfor man skal ha tilgang til bestemte data/opplysninger. Et eksempel kan være helserelatert: en doktor får tilgang opplysningene om personene han/hun skal behandle den dagen.

Talleraas utdyper bruk av attributtbasert-tilgangskontroll; - *I hovedsak er tilgang til saker og informasjon behovsstyrt, dvs at saksbehandler får tilgang til informasjon som har med de enkelte saker som saksbehandleren har med å gjøre. Denne tildelingen av saker kan gjøres eksplisitt (ved direkte tildeling av sjef/andre med rettigheter) eller implisitt avhengig av stilling, arbeidssted og organisasjonstilhørighet. Man kan også se for seg løsninger der saksbehandler spør om tilgang, men dette har ikke vært videre diskutert.* Videre fortsetter han om krav til sporing; - *I tillegg til tilgangs-kontroll har Skatteetaten krav til sporing, dvs dokumentasjon av hvilke brukere som har sett på hvilke data, men dette gjelder først og fremst sensitiv informasjon (for eksempel hemmelig adresse)*

Rollebasert autentisering

Skatteetaten og Difi benytter seg av rollebasert tilgangskontroll på applikasjonsnivå. Difi benytter roller for å begrense tilgang til personopplysninger og data. Dette gjelder også Skatteetaten, men gjennom ATS-prosjektet(Attributtbasert tilgangsstyring), innføres også attributt-/policy-basert tilgangskontroll. Dette fordi rollebasert tilgangskontroll ikke er tilstrekkelig for å implementere de kravene og reglene Skatteetaten har til tilgangsstyring.

Datatilsynet argumenterte for at tilsynsavtaler er et alternativ for å sikre adgangskontroll for store registre. Eksempelvis kan det i forhold til IdMegler utvikles en tilsynsavtale mellom register og virksomhet. I tillegg er man avhengig av at virksomhetene som benytter IdMelger har god tilgangsstyring, samt et klart skille i autentiseringen av brukere i systmene.

Skytjeneste (Cloud)

Difi og Skatteetaten beskriver skytjenester som spennende utfordringer for fremtiden. Skatteetaten trekker frem at norske personopplysninger (red.anm definert i følge Personopplysningsloven) kun kan lagres der norske lover gjelder. Dersom skytjenester skal kunne benyttes av offentlige virksomheter, må dette være norske skyer. Eksempelvis har Evry valgt å outsource drift og vedlikehold av systemene for ulike banker til utlandet, men de må fremdeles lagre opplysningene/data i Norge[78],[79].

[78] Digi: Sveinbjørnsson, Evry vil sende driften ut av landet, www.digi.no, http://www.digi.no/902573/evry-vil-sende-driften-ut-av-landet, 19.09.2012, 29.01.2013

[79] Computerworld: Lyse, It-sjef slo alarm om bank-inntrengere, www.idg.no, http://www.idg.no/computerworld/article162809.ece, 29.03.2010, 29.01.2013

Difi trekker frem flere problemområder med skytjenester relatert til sikkerhetsmekanismer, samt tilgjengelighet og konfidensialitetsbrudd. I tillegg ser både Difi og Skatteetaten utfordringer med kontroll over informasjon og opplysninger som er lagret i skyen.

Skatteetaten ser videre for seg muligheten for gjennomføre saksbehandling i skyen. Da vil det være høyt fokus på at skyen ikke "lekker" informasjon eller opplysninger, det vil si at den tilfredstiller alle krav satt til sikkerhet. Her kan det også være et alternativ å ta i bruk en privat sky.

Tjeneste-orientert arkitektur

Skatteetaten og Datatilsynet ble spurt om hvordan tjeneste-orientert arkitektur kan forbedre anonymiseringen av personopplysninger i forhold til Personopplysningsloven og Forskningsspørsmål 1.

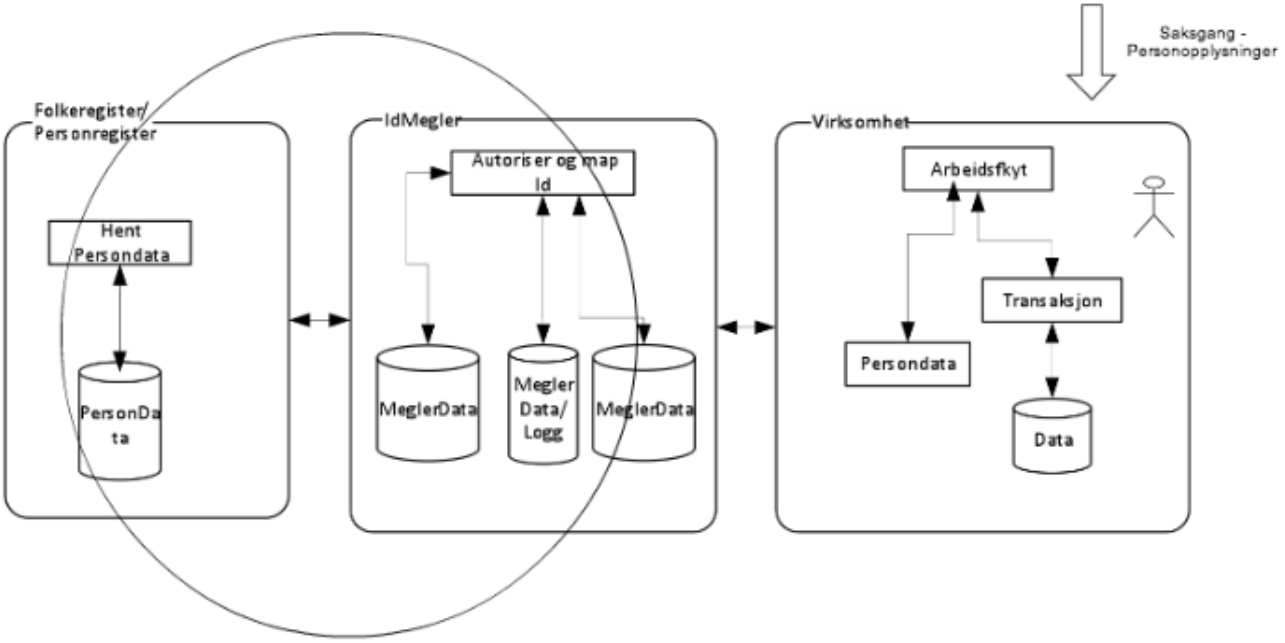
Skatteetaten argumenterte for at tjeneste-orientert arkitektur kan øke personvernet ved at virksomhetene lagrer og tilbyr egne tjenester, og ikke sender kopier av data/registre til andre virksomheter som forvalter og behandler data for dem. Da har virksomheten som oppbevarer registeret mulighet til å benytte logging og se hvem som har gjort hva i ettertid - kontroll.

Datatilsynet trekker frem eksempler hvor det vil være hensiktsmessig å duplisere data og registre. I noen tilfeller blir systemkravene for høye til at virksomhetene klarer å behandle dem selv. Dette kan for eksempel være i forbindelse med NAV sin utbetaling av trygd, eller ved utsendelse av selvangivelser. Her settes store krav til tilgjengelighet, oppetid, sikkerhet og tilgangsstyring (nivå 4).

5.2.2 Perspektiver på IdMegler

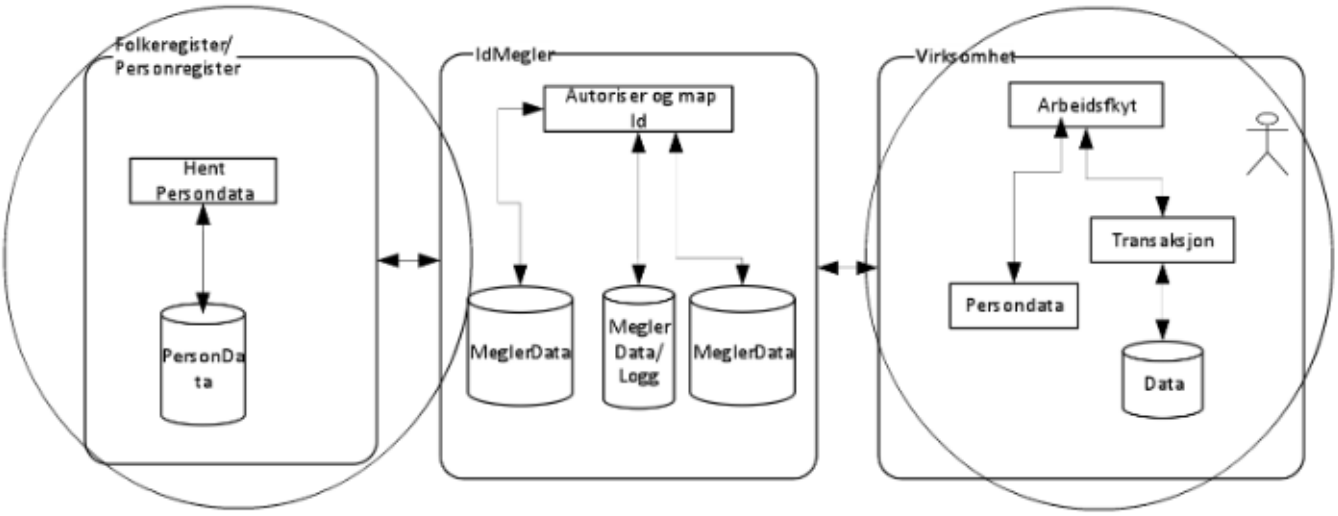
Under dybdeintervjuene ble representantene fra virksomhetene presentert for IdMegler-arkitekturen. Målet med arkitekturen, samt samfunnsmessige behov og gevinster ved innføring av den. Virksomhetene hadde ulike fokusområder, avhengig av virksomhetens fagområde, og så ulike utfordringer ved innføringen av en slik løsning.

Figur 5.1 viser Skatteetaten sitt fokusområde ved diskusjon rundt IdMegler. Skatteetaten valgte å trekke frem Personregisteret og IdMegler for så å sammenligne disse med egne systemer under utvikling (se Kapittel 5.2.2). Videre belyste Skatteetaten problemer og utfordringer vedrørende behandling og lagring av Personopplysninger som oppstår gjennom saksbehandling i virksomheter.



Figur 5.1: Skatteetatens fokusområde ved diskusjon rundt IdMegler

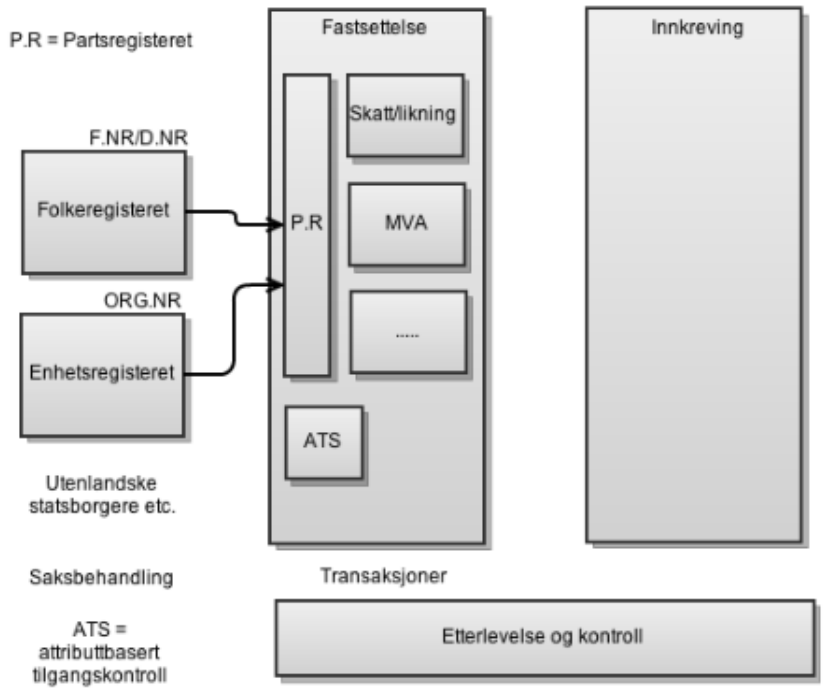
Difi og Datatilsynet valgte et annet fokusområdet og konsentrerte seg om Personregisteret og virksomheten, som vist i Figur 5.2. Datatilsynet tok utgangspunkt i lovverket og hvordan IdMegler arkitekturen kunne utnyttes tilfredstillende. Difi valgte å fokusere på sikkerhetsaspektet rundt koblingene mellom Personregisteret og IdMegler, samt IdMegler og virksomhet.



Figur 5.2: Difis og Datatilsynets fokusområde ved diskusjon rundt IdMegler

Skatteetatens perspektiv på IdMegler

Figur 5.3 viser en overordnet skisse av Skatteetatens systemer, og et utdrag av prossessflyten for saksbehandling. PR viser det beskrevede Partsregisteret og ATS representerer den attributtbaserte tilgangskontrollen. Som Figuren viser, deles personopplysninger fra Folkeregisteret, Enhetsregisteret og andre kilder til Partsregisteret, som sammen med ATS blir utviklet i oppgraderingen av Skatteetatens systemer.



Figur 5.3: Overordnet Figur over Skatteetatens systemer, utdrag av prosessflyt for saksbehandling.

En av utfordringene framover er at dagens fødselsnummer-ordning mest sannsynlig vil bli endret som en del av Folkeregister-moderniseringen. Skatteetaten må dermed bygge de nye systemene robuste nok til at endringene i Folkeregisteret ikke medfører større endringer i skatte- og avgiftssystemene. I Partsregisteret vil derfor hver person lagres som et objekt med en individuell nøkkel som ikke er meningsbærende.

IdMegler kan ses på som Skatteetatens Partsregister og ATS. Hvor IdMegler er tilgangskontrollen med nøkkelhåndtering, og Partsregisteret, den autorative kilden til personopplysninger.

Datatilsynets perspektiver på IdMegler

IdMegler-arkitekturen kan kun tas i bruk dersom både registeret og virksomhetene, som benytter det, er offentlige virksomheter (red.adn En offentlig virksomhet er et organ som har mulighet til å forbedre og/eller fatte forvaltningsvedtak etter reglene i Forvaltningsloven[80],[81]). Dette er begrunnet

[80]Lovdata, LOV-1967-02-10: Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven), www.lovdata.no, http://www.lovdata.no/all/nl-19670210-000.html, 10.02.1967 , 04.03.2013
[81]Skatteetaten, Utlevering av opplysninger til offentlige myndigheter, www.skatteetaten.no,

gjennom lovverket, og det er lovlig gunnlag for deling dersom det finnes paragrafer i enkeltlover som sier at informasjon kan utleveres eller innhentes. Altså er samtykke ikke eneste behandlingsgrunnlag for noe kan deles også uten samtykke. Evt. finnes det eksempler hvor virksomheten er privat (red.anm Ovenfor private virksomheter er opplysningene i DSF underlagt taushetsrett, begrenset taushetsplikt og taushetsplikt[82]), for eksempel inkasso- eller eiendomsvirksomheter.

Ved kobling mellom register og virksomhet, vil IdMegler opptre som en databehandler. Databehandleren kan kun gjøre akkurat det den er blitt forespurt av register eller virksomhet. Det vil si at offentlige virksomheter kun kan ta i bruk databehandlerens funksjonalitet som er godkjent av Datatilsynet. Datatilsynet kan gjøre tilsyn/vedtak mot enhver virksomhet som tar i bruk databehandleren og benytter den i samspill med personopplysninger.

Eksempelvis vil IdMegler ved kobling mot Folkeregisteret få tilgang til å hente opplysninger ved dokumentert datagrunnlag, som behandlingsansvarlig (forutsetter at registeret og virksomheten er offentlig).

5.3 Dybdeintervju: Privat virksomhet

Sparebanken 1-gruppen og Statoil er begge virksomheter i privat sektor, innenfor henholdvis bank- og oljebransjen.

5.3.1 Tematisk sammenfatting av dybdeintervju med Sparebanken 1-gruppen

Personopplysninger

Sparebank 1-gruppen er et holdingselskap og har personopplyninger lagret relatert til marked, bank og forsikring. I bankene er det lagret lite sensitive personopplysninger (ref. Personopplysningslovens definisjon av personopplysninger), mens det i forsikring er lagret en mye større andel sensitive opplysninger. For eksempel i forbindelse med helse og ved behandling av livsforsikringsgrunnlag.

Sparebanken 1-Gruppen har mange systemer, og håndterer derav store mengder kunde- og personopplysninger. Personopplysninger flyter ofte mellom de ulike systemene i en bedrift, mens det er begrenset flyt mellom de ulike selskapene. Dette begrenses av Personopplysningsloven og Finansloven (konkurranse mellom de ulike bankene).

Det benyttes vasking av databaser mot offentlige registre (blant dem DSF) for å kvalitetsikre lagrede personopplysninger.

---

http://www.skatteetaten.no/no/Person/Folkeregister/Utlevering-av-opplysninger/Folkeregisteropplysninger/Utlevering-av-folkeregisteropplysninger-til-offentlige-myndigheter/, ukjent, 04.03.2013.

[82] Skatteetaten, Utlevering av opplysninger til private, www.skatteetaten.no, http://www.skatteetaten.no/Person/Folkeregister/Utlevering-av-opplysninger/Folkeregisteropplysninger/Utlevering-av-folkeregisteropplysninger-til-privatpersoner-og-institusjoner/, ukjent, 04.03.2013

Felles register

Sparebanken 1-Gruppen jobber i dag med å sette opp et felles internt register for kontaktinformasjon basert på master data-tankegang, presentert i kapittel 5.3.2.

I dagens systemet vaskes personopplysninger mot DSF, opptil flere ganger per kunde. Målet med et nytt register er å synkronisere personopplysninger så langt det lar seg gjøre. I utgangspunktet gjelder dette kontaktinformasjon. Registeret blir opprettet med begrensninger, men det vil ikke erstatte dagens løsninger. Det vil heller ses på som et felles oppdateringspunkt, med økt kvalitet på lagrede personopplysninger. Løsningen vil også senke dagens vedlikeholdskostnader og antall synkroniseringer mot DSF.

Med innføring av nye løsninger, er det ønskelig å trekke ut oppdatering og vask mot offentlige register fra fagsystemene.

Fordelen ved å benytte et felles register er økt datakvalitet og kostnadsreduksjon ved å redusere antall sjekk av data mot offentlige registre. I tillegg muliggjøres Id-kobling uten bruk av personnummer (I forhold til Forskningsspørsmål 3).

Det vil i fremtiden være mulig å benytte systemer uten lokale personregistre, men dette krever standarder og endring av allerede eksisterende systemer. En mulig løsning kan være en blanding mellom IdMegler og et master data system. I noen systemer vil det være vanskelig å ikke forvalte egne registre. For eksempel ved kundeoppfølging, hvor man er avhening av å kunne kartlegge demografisk filtrering, utfordringer med disse og bruksmønster.

Lagring av personopplysninger

Personopplysninger må ikke være tilgjengelig for alle fagsystemer, dette varierre fra system til system, men personopplysninger ligger i stor grad lagret i fagsystemene. Det vil også være duplikater av personopplysninger i systemene, noe som er umulig å unngå, fordi mange av de gamle systemene (kjernesystemene) må ha tilgang til personopplysninger. Duplikatene oppdateres ved automatisk synkronisering internt i systemene og benyttes i størst grad på tvers av de ulike virksomhetene i gruppen (ref. lovgivning).

Innsyn i personopplysninger

Innsynsforespørsler kommer til bankene og hver enkelt bank "eier" rutinen for å håndtere en innsynsforespørsel. Bankene samarbeider om rutinene, men de kan variere fordi det er stor forskjell på bankene i alliansen. Hver enkelt bank har konsesjon for behandling av personopplysninger. Det vil si at Sparebank 1-gruppen fungerer som databehandler og gjennomfører prosjektene og oppgaver bankene etterspør.

Skytjeneste (Cloud)

Sparebank 1-Gruppen vil per dags dato ikke benytte seg av skytjenester. Lagring av personopplysninger utenfor Norge er strengt regelbelagt og kundedata skal alltid lagres i Norge.

Tjeneste-orientert arkitektur (FS1)

Aasen argumenterer for at det i mange tilfeller vil være realiserbart med en arkitektur som IdMegler, men det vil også være vanskelig for en del systemer, feks. bank. Samtidig vil det være en stor fordel å kun beholde transaksjonene i fagsystemene og kundeopplysninger i et annet register.

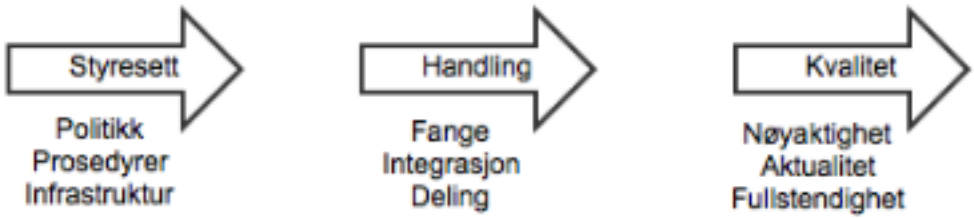
En av de største utfordingene er definisjonen av personoppplysninger. I banksammenheng er kontonummer også en personopplysning, og kontonummeret er lett å knytte til person. Her er det viktig å se på hva som knytter dataene til personene. Dersom noen data er knyttet til en person en gang, hvordan sikrer man at dette skjer/ikke skjer igjen? Dette vil også gjelde for distribusjon av personnøkkel i systemene. Aasen mener at økt personvern handler om hvordan man kan sikre at identifikatoren ikke bryter anonymiteten.

Sparebank 1-gruppen sine perspektiver på IdMegler

Ved introduksjon til IdMegler påpekte Aasen at noen av prinsippene i arkitekturen kunne knyttes til *Master Data Management*.

5.3.2 Introduksjon til Master Data Mangement

Masta Data Management (MDM) betegnes som en samling av *Best Data Management* praksis. MDM opptrer som en aktiv bidragsyter i organiseringen av nøkkelinteressenter, -deltakere og -forretningsklienter. Herunder inkluderers forretningsapplikasjoner, informasjonsmetoder og *Data Management Verktøy*. Disse benyttes for å implementere verktøy for retningslinjer, prosedyrer, tjenester og infrastruktur for å støtte integrasjon, konsistente og komplette masterdata (Loshin, 2009). Som vist i Figur 5.4, tas det hensyn til styresett (Governance), handling (Action) og kvalitet (Quality).



Figur 5.4: Illustrasjon (oversatt til norsk) av MDM, Master Data Mangement (Loshin, 2009)

Et MDM program har som intensjon å støtte en organisasjonsforretnings behov ved å tilby tilgang til konsistente syn på unikt identifiserbare *Master Data* enheter på tvers av operasjonell applikasjonsinfrastruktur.

5.3.3 Tematisk sammenfatting av dybdeintervju med Statoil

Personopplysninger

Personopplysninger er et bredt begrep og omfavnet mer enn personlige opplysninger om en person. Det er også personens handlingsmønster, væremåte, for eksempel personens bevegelsesmønster på nett, eller hvilke filmer personen så på firmareise. Det er derfor viktig å ha fokus på alle opplysninger som kan knyttes til en person, og ikke nødvendigvis bare navn, personnummer og informasjon om inntekt.

Felles register

Wesenberg ble spurt om det ville være mulig og hensiktsmessig å opprette en felles kilde til personopplysninger i fremtiden. Et felles register vil føre til utfordringer i forbindelse med sikring og kompleksitet. I tillegg vil det være en utfordrende tilgangsstyringsprosess. Dersom et felles register skal opprettes bør kun felles opplysninger for alle virksomhetene som benytter det lagres i registeret. Det er viktig å ta hensyn til at all informasjon lagret i store registre en gang blir offentlige opplysninger.

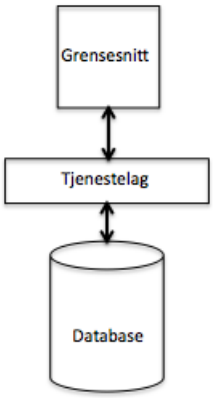
Wesenberg argumenterer videre for at det i mange tilfeller vil være bedre å bygge registre mot bruk. Fordi det nettopp vil være tilpasset bruk og dermed kan tilby høy og tilfredstillende kvalitet på opplysningene lagret i registeret.

Skytjeneste (Cloud)

Statoil benytter seg daglig av Amazons skytjenester, men ikke til lagring av personopplysninger og har god erfaring ved bruk av disse.

Tjeneste-orientert arkitektur (FS1)

Tjeneste-orientert arkitektur vil definitivt øke personvernet fordi man begrenser tilgang til informasjon og opplysninger lagert i databasen, ved å opprette et tjenestelag. Gjennom tjenestelaget kan man sette retningslinjer og gjennom grensesnitt kan det tilbys bestemte spørringer. Ved hjelp av en tjeneste-orientert arkitektur kan man skjule innsynsvinkler for brukerne, og på den måte igjen hindre tilgang til data som ikke skal ses i sammenheng. Figur 5.5 viser hvordan grensesnittet og spørringene begrenser tilgang til registrene lagret i databasen.



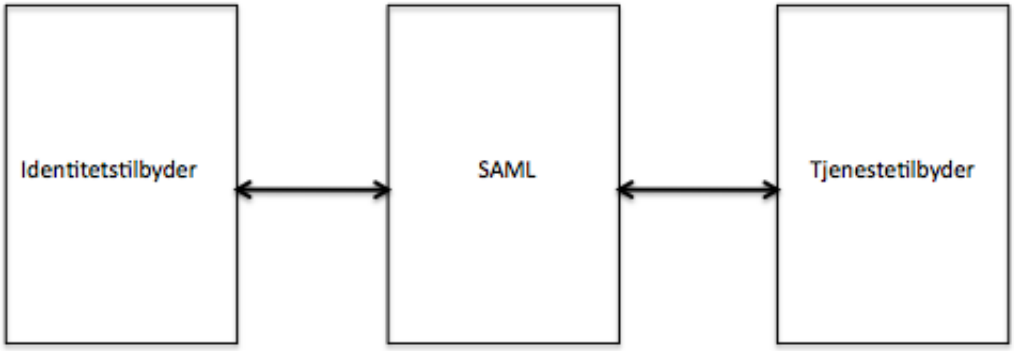
Figur 5.5: Illustrasjon av tjeneste-orientert arkitektur

Statoil sine perspektiver på IdMelger

Ved introduksjon til IdMegler-arkitekturen påpekte Wesenberg at Statoil allerede benytter en lignende arkitektur og standard, SAML.

5.3.4 Introduksjon til SAML

SAML (Security Assertion Markup Language) versjon 2.0 er en godkjent OASIS Standard fra mars 2005[83]. SAML er en XML-basert, åpen standard for utveksling av data, autentisering og autorisasjon mellom partnere, spesielt mellom leverandør og tjenesteleverandør/klient og tjener (Lewis, 2009). Figur 5.6 viser en overordnet illustrasjon av SAML, og forholdet mellom identitetstilbyder og tjenestetilbyder.



Figur 5.6: Illustrasjon av overordnet SAML-arkitektur

Figur 5.7 viser flytdiagrammet for nettbasert bruk av SAML. Som Figuren viser definerer SAML forespørsel- og tilbakemeldingsprotokoller (request and respons protocols), brukt for kommunika-

[83]OASIS, SAML Specifications, www.saml.xml.org, http://saml.xml.org/saml-specifications, ukjent, 14.03.2013

sjon mellom tjenestetilbyder og identitetstilbyder. Videre mapper SAML bindingene protokollene til lavere nettverkskommuikasjonsnivå protokoller som brukes for å transportere SAML påstander mellom identitetstilbyder og tjenestetilbyder (Lewis, 2009).

Figur 5.7: Illustrasjon (oversatt til norsk) av arbeidsflyt for nettbasert SAML (Lewis, 2009)

1. Forespørsel om ressurs, 2. Autentiseringsforespørsel, 3. Brukerpålogging, 4. HTML SAML signert eller kryptert tilbakemelding, 5. Nettleser POST SAML tilbakemelding, 6. Tjenestetilbyder sikrer godkjenning og autorisasjon fra SAML, 7. Nettressurs levert.

SAML kan benyttes som en standard for autentiseringskontroll. Standarden tilbyr sertifikater som avgjør om brukeren skal være autentisert for prosessen som blir forespurt av virksomheten/tjenestetilbyder, basert på informasjonen levert av identitetstilbyder. Ved bruk av SAML kan man tilby tilgangsstyring til applikasjoner utenfor egen virksomhet, uten å gi tilgang til, eller gi fra seg, personopplysninger.

Det finnes mange likhetstrekk mellom IdMegler og SAML, både i forhold til arkitektur og autentisering/klient-tjener tankegang. Den største forskjellen er IdMeglers kobling til det autorative personregisteret. SAML er en protokoll og tilbyr en handshake mellom ulike applikasjoner. Dermed kan SAML benyttes for autentisering ved bruk av IdMegler, men protokollen vil ikke ha noe forhold til logg og innsyn.

5.4 Scenarioer

Det vil basert på dybdeintervjuene og tilbakemeldingene vises til ulike scenarioer for dagens løsninger, samt mulig endringer og forbedringer ved innføring av IdMegler.

5.4.1 Sensitive personopplysninger

Scenario: Sensitive personlige opplysninger om en person, gjennom helsejournaler blir spredt.
Problemområde: Skaden kan i liten grad rettes opp. Sensitive personopplysninger gis under tillit og fortrolighet – brudd på tillit kan medføre alvorlig tillitskrise.
Risikovurdering: Sannsynlighet, *Stor*. Konsekvens, *Stor*.

Spredning av sensitive helseopplysninger innebærer brudd på forventet diskresjon og kan føre til alvorlig tillitsbrudd mellom individ og virksomhet, her lege og pasient. I et slikt tilfelle kan informasjonen og evt journalene bli lekket eller enda verre, lagt ut på nett tilgjengelig for søk, åpent for alle.

Spredning av fortrolig informasjon kan også relateres til bærebare datamaskiner på ulike arbeidsplasser. Videre kan åpne nett være en årsak til spredning av sensitive personopplysninger.

Ved bruk av IdMegler-arkitekturen ville ikke personopplysningene vært lagret lokalt og personopplysningene vil vært skilt ut fra helse-historikk. Dette ville ført til høyere sikkert og lavere risiko for misbruk og tillitsbrudd, samt en høyere grad av anonymisering for personen det gjelder. Spesielt siden benyttet ID ikke kan knyttes til person direkte.

5.4.2 Spredning av personopplysninger

Scenario: Personopplysninger om en person blir spredd ved en feil, ref. Kenneth sin selvangivelse[84].
Problemområde: Skaden kan i liten grad rettes opp.
Risikovurdering: Sannsynlighet, *Stor*. Konsekvens, *Stor*.

Noen personopplysninger blir spredt ved en feiltakelse og andre blir solgt uten den enkeltes samtykke til f.eks. reklame og analyse av forbruksmønster. Det vil si at personen det gjelder ikke har nok kunnskap til å vite hva som skjer med personopplysningene lagret hos en virksomhet. I noen tilfeller vil det også være slik at enkeltpersoner ønsker å spre personopplysninger om seg selv.

Ved elektronisk visning av selvangivelsen på Altinn de siste årene, har det vært store sikkerhetsproblemer, noe som ført til at personer ved innlogging har fått tilgang til andre personers profil og informasjon. I 2012 gikk dette utover Kenneth, og i 2013 fikk flere brukere tilgang til Eirik sin bruker og selvangivelse[85]. Dette har ført til at personinformasjon har blitt spredd ved en feil, og kan få store konsekvenser for dem det gjelder. Omfanget av slike feil er vanskelig å avklare helt sikkert, men skaden øker eksponentielt med antall personer som blir rammet av feilen.

[84] E24; Landre, - Hvis ikke Kenneth er fiktiv, så har Altinn et stort problem, www.e24.no, http://e24.no/digital/hvis-ikke-kenneth-er-fiktiv-saa-har-altinn-et-stort-problem/20176285, 20.03.2012, 19.03.2013

[85] Dagbladet: Thorvaldsen, Ny Altinn-tabbe: Eirik fikk opp fremmed navn og personnummer, www.dagbladet.no, http://www.dagbladet.no/2013/03/19/nyheter/innenriks/altinn/26295539/, 19.03.2013, 21.03.2013

Ved en implementering av IdMegler, vil det muliggjøre at personer til enhver tid kan sjekke hvilke virksomheter som har opplysninger knyttet til personen (hvem), hvilke opplysninger som er registrert (hva), hvilke formål (prosesser) opplysningene er benyttet i (hvorfor) og når opplysningene er benyttet. Videre vil det være et fysisk splitte mellom identifiserende personopplysninger og saksbehandlingsdata knyttet til person. Disse vil kobles gjennom arbeidsprosesser, og tilgangen til kobling vil være tidsbegrenset og knyttet til startet saksbehandling og avluttes i arbeidsprosessen.

5.4.3 Unix-passordfiler

Scenario: De fleste UNIX-systemer lagrer informasjon om brukeren i to filer, */etc/passwd* og */etc/shadow,* for bruk ved autentisering og innlogging[86].
Problemområde: Alle brukere kan lese den krypterte passord-filen.
Risikovurdering: Sannsynlighet, *Middels*. Konsekvens, *Stor*.

I filen */etc/shadow* finnes informasjon om brukernavn, brukeridentifikasjon og ukrypterte passord. Mens filen */etc/passwd* er tilgjengelig for alle brukere, og inneholder brukernavn, brukeridentifikasjon og kryptert passord. Informasjonen brukes i forbindelse med innlogging og autentisering til systemet.

Dette er et eksempel på gammel teknologi, og at det er uheldig å benytte samme løsning til autentisering og autorisasjon. Det kan trekkes paralleller til bruk av LDAP (Lightweight Directory Access Protocol) og AD (Active Directory). LDAP er en applikasjonsprotokoll for tilgangstyring og vedlikehold av distribuerte katalogtjenester over et internett-protokoll(IP)-nettverk[87], mens AD er katalogtjeneste utviklet av Microsoft for Windows domene systemer, og inneholder Windows server operativsystemet[88]. LDAP brukes for autentisering av brukere og inneholder beskrivende attributter for alle autentiserte brukere. I tillegg utvikles det detaljerte krav og retningslinjer for kobling mellom applikasjoner og bruk av protokollen. AD benyttes til å administrere identiteter og oppretter relasjoner mellom distribuerte ressurser slik at de kan fungere sammen.

En mulighet for fremtiden vil være å bytte ut katalogtjenestene med IdMegler-arkitekturen. Dette vil ikke bare øke personvernet, men også heve sikkerheten rundt systemene.

5.4.4 Skytjenester (Cloud)

Scenario: En offentlig virksomhet ønsker å benytte seg av en leverandør av skytjenester.
Problemområde: Innebærer en overføring av personopplysninger fra virksomhet til leverandør.
Risikovurdering: Sannsynlighet, *Middels*. Konsekvens, *Stor*.

Personopplysninger om norske statsborgere kan ikke lagres utenfor Norges grenser. Skytjenester kan benytte for lagring av personopplysninger dersom de er offentlige og norske. Det er også mulig å

[86] Itsavvy, Unix Password File, www.itsavvy.in, http://www.itsavvy.in/unix-password-file, ukjent, 17.03.2013
[87] University of Michigan; Howes, The Lightweight Directory Access Protocol: X.500 Lite, www.openldap.org, http://www.openldap.org/pub/umich/ldap.pdf, 27.07.1995, 21.03.2013
[88] Windows server, Active Directory Collection, www.technet.microsoft.com, http://technet.microsoft.com/en-us/library/cc780036(WS.10).aspx#w2k3tr_ad_over_qbjd, 01.06.2011, 21.03.2013

frikoble personopplysninger fra sakbehandlingsdata og gjennomføre sakbehandlingprosessen i skyen. Da vil det ikke settes krav til at skyen er norsk.

Dersom en virksomhet ønsker å flytte saksbehandlingsprossen til skyen kan IdMegler opptre som en meglingstjeneste og opprette koblinger mellom saksbehandlingsprosessen og personopplysningene lagret i et personregister. På den måten sikres personens rettigheter og personopplysninger.

5.4.5 Tilgangsstyring evt. Tjeneste-orientert arkitektur

Scenario: NAV sitt AA-register inneholder navnelister over ansatte i etterretningstjenesten[89].
Problemområde: Hemmligstemplet og gradert, sensitiv informasjon lå åpent for søk blandt 38.000 offentlig ansatte.
Risikovurdering: Sannsynlighet, *Middels*. Konsekvens, *Stor*.

NAV oppbevarer i dag et register med informasjon om hvem som er ansatt hvor i Norge. Dette er en oversikt over alle norske bedrifter og deres ansatte, inkludert etterretningstjenesten. Registeret heter AA-registeret og nærmere 40.000 offentlig ansatte har tilgang til det.

Begrensning av tilgang til informasjon, situasjons- og rollerbasert tilgangsstyring kunne vært med på å begrense spredningen av hemmeligstemplet informasjon. Et *åpent* register er en risiko i seg selv, med tanke på utro tjenere, og lovbrudd både med hensikt og uten hensikt.

Det vil ved bruk av IdMegler vil det være et fysisk skille mellom personopplysningene, sakbehandlingen og saksbehandlingsdata. Dermed kan ikke opplysninger i registeret benyttes for å finne annen opplysninger knyttet til person. Videre vil IdMegler gi økt kvalitet og sikkerhet på de lagrede opplysningene, samt logging, som kan brukes for kontroll. Dette ville begrenset tilgangen og øke kontrollen og personvernet til hemmeligstemplet og gradert, sensitiv informasjon i AA-registeret, og derav en høyere grad av personvern for den enkelte.

5.4.6 Autorisasjon

Scenario: Bruker ønsker å logge inn på en offentlig portal, som f.eks. Altinn, Lånekassen eller ID-Porten ved hjelp av MinId eller BankId.
Problemområde: Det skjer en feil i innloggingsprosessen som medfører at brukeren får tilgang til andre brukerprofiler enn sin egen.
Risikovurdering: Sannsynlighet; *Middels*. Konsekvens; *Stor*.

Innlogging i Altinn skjer ved hjelp av en totrinns autorisasjon[90]. Ved innlogging til Altinn gjennomføres først en autentisering ved bruk av sluttbrukersystemID og tilhørende passord. Videre vil det være behov for å autentisere den unike brukeren som benytter sluttbrukersystemet og autorisere at vedkommende har rettigheter til å levere eller hente spesifikke data eller utføre operasjoner. Dette

[89] Aftenposten, Ansatte i e-tjenesten i offentlig register, www.aftenposten.no, http://www.aftenposten.no/nyheter/iriks/article3629704.ece#.UUWupetqPbY, 12.10.2011, 17.03.2013
[90] Accenture og Altinn; Implementasjonsguide for sluttbrukersystemer, www.altinn.no, https://www.altinn.no/upload/1500/Implementasjonsguide%20for%20sluttbrukersystemer.pdf, ukjent, 21.03.2013.

gjøres ved hjelp av engangskode som referer til hvilken prosess som skal startes. Det startes en prosess basert på forretningsbehov. Prosessen vil være gyldig i en halv time, og må fornyes for å ikke løpe ut.

IdMegler kan benytte MinId eller BankID for innlogging og kan tilby kobling mellom f.eks Altinn og et overordnet personregister.

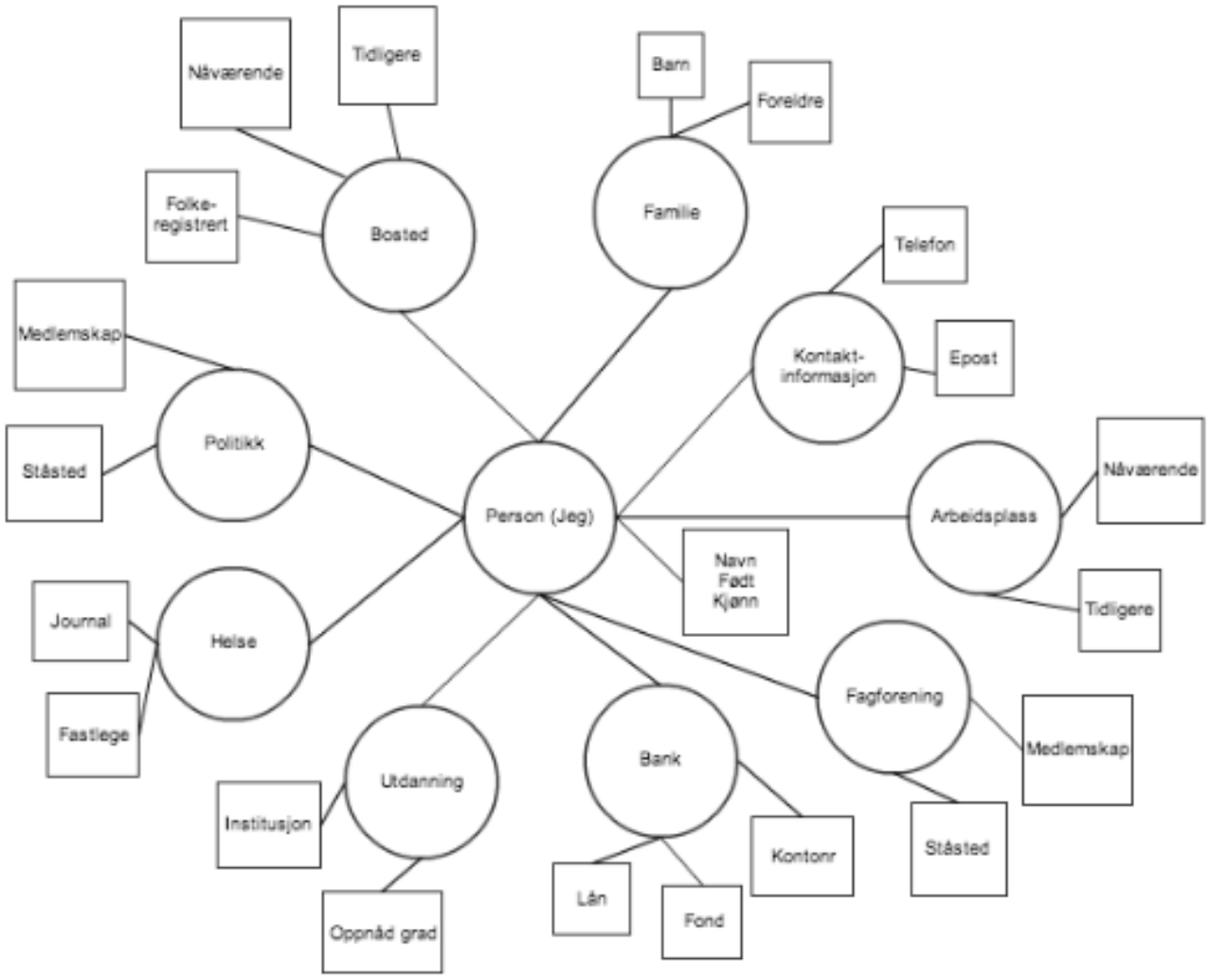
5.4.7 Bruk og gjenbruk av brukernavn og passord

Scenario: En brukers profil blir hacket.
Problemområde: Brukeren har benyttet samme brukernavn og passord på flere innloggingstjenester, feks. nettbank, mailtjenester, sosialemedier osv.
Risikovurdering: Sannsynlighet, *Stor*. Konsekvens, *Stor*.

Nesten alle hjemmesider eller nettjenester har sin egen innlogging i dag. Dette fører i stor grad til gjenbruk av brukernavn og passord. Facebook og Google har tatt i bruk en løsning som gjør at innlogging på mange sider kan skje gjennom dem. Problemet er her at innlogging baseres på unike brukere, ikke på unike personer, dvs. falske profiler. En føderert løsning ved bruk av f.eks. MinID vil være en mulighet for fremtiden. Dette vil videre føre til en nedgang i antall personregistre lagret hos ulike virksomheter, samt at det gir brukerne mulighet til å vite hvilke informasjon som blir lagret. En føderert løsning vil være en mer sikker identitetskilde, og vil i en større grad ivareta integriteten til den enkelte, samt øke personvernet til den enkelte.

Id-Megler kan bidra til å redusere antall registre, ved integrasjon med et overordnet register og en innloggingstjeneste. En slik løsning vil også bidra til høyre kvalitet på lagret informasjon og i høyre grad muliggjøre brukerkontroll og oversikt. Det kan også være en fordel å utvikle brukernavn og passord som ikke er menings- eller kontekstbærende. Dette vil ikke direkte redusere faren for hacking, men det vil sikre personopplysningene, og gi mindre muligheter for kobling av personopplysninger.

Figur 5.8 viser mange av personopplysningsrelasjonene til en person, og hvordan det kan finnes store og mange registre lagret hos ulike virksomheter.



Figur 5.8: Registerrelasjon av personopplysninger for en person.

5.4.8 Identitetstyveri

Scenario: En person sender ut en mail og utgir seg for å være en stor bank. E-posten sendes ut til en rekke personer og opplyser for eksempel om at det er problemer med kredittkort fra banken. Problemet kan imidlertid, ifølge e-posten, løses lett ved å følge en vedlagt lenke til en nettside, svare på spørsmål og fylle inn personalia og kredittkortinformasjon. Informasjonen brukes til å tappe kredittkortet for penger.
Problemområde: Misbruk av personopplysninger for å fremme et ulegitimt formål, f.eks å skaffe seg tilgang til og kontroll over andres øknomiske midler, kredittinstrumenter eller eiendom.
Risikovurdering: Sannsynlighet, *Middels*. Konsekvens, *Stor*.

Phishing eller digitalsnoking handler om fisking etter personopplysninger eller konfidensiel informasjon som passord, brukernavn og kredittopplysninger. På den måten kan en annen person ta kontroll over dine kredittinstrumenter.

Identitetstyveri dømmes som et brudd på Straffelovens § 190a[91], *Det er straffbart å bruke en annen persons identitet eller en identitet som er lett å forveksle med en annens identitet for å oppnå en uberettiget vinning eller påføre noen et tap eller ulempe.*

Høyere kjennskap og fokus knyttet til personvern og bruk av egne personopplysninger blandt innbyggerne i Norge, vil gi en lavere risiko knyttet til identitetstyveri og phishing. Videre kan bruk av et felles register medføre at virksomhetene eller tjenestene ikke trenger å spørre om personopplysninger. Det er også mulig å opprette koblinger som gjør at bankkort ikka kan benyttes uten kobling til personregisteret. Dette vil i stor grad kunne være med å redusere faren for identitetstyveri.

[91]Lovdata, LOV 1902-05-22 nr 10: Almindelig borgerlig Straffelov (Straffeloven), www.lovdata.no, http://lovdata.no/all/tl-19020522-010-022.html#190a, 22.06.2012 ,18.03.2013

5.5 Sammendrag

- Dybdeintervjuene viser at det er mulig å se likheter og ulikheter mellom virksomhetene, men også mellom de ulike bransjene og sektorene. Alle de intervjuede virksomhetene behandler og lagrer store mengder personopplysninger. Dermed har de et forhold til lagring, bruk av og sletting av personopplysninger. Virksomhetene må også forholde seg til lover, regler og normer, og er igjen knyttet til andre virksomheter.
- Lagring og sletting av personopplysninger er hovedsaklig regulert av lovverket, hovedsaklig Personopplysningsloven, men i noen tilfeller også Arkivloven og Bokføringsloven.
- Personopplysninger lagres i fagsystemene, grunnet behovet for tilstedeværelse av personopplysninger gjennom saksgang.
- Alle virksomhetene har retningslinjer for behandling av innsynsforespørsler.
- Det er uenighet rundt fordelen ved innføring av et felles personopplysningsregister, og hvorvidt tjeneste-orientert arkitektur vil gi økt personvern for den enkelte, dette vil bli diskutert videre i kapittel 6, Diskusjon.

For å få en overordnet oversikt av dybdeintervjuene er det utviklet en sammenfattende tabell, tabell 5.1 inneholdene de ulike hovedtema. Tabellen sammenligner NTNU, offentlig og privat sektor. Svarene er basert på NTNU sitt FS (Felles student system), Offentlig sektor omfatter Skatteetaten sitt PR og ATS (Partsregister og attributtbasert tilgangstyring), samt DIFI sin ID-Port. Privat sektor baserer seg på Sparebanken 1-gruppen og Statoil sine overordnede retningslinjer for personvern og arkitektur.

	NTNU - FS	*Offentlig sektor*	*Privat sektor*
Personopplysninger	Opplysninger om personen og opplysninger relatert til forholdet til NTNU.	Definert gjennom Personopplysningsloven.	Definert gjennom Personopplysningsloven.
Sensitive personopplysninger	Delvis	Ja	Ja
Innsyn	Ved forespørsel. Følger retningslinjer og lovpålagte regler.	Ved forespørsel. Følger retningslinjer og lovpålagte regler.	Ved forespørsel. Følger retningslinjer og lovpålagte regler.
Sletting/lagring	Ingen opplysninger i systemet slettes, status til personen endres.	Ingen opplysninger slettes, da mange virksomheter i offentlig sektor har unntak fra lovverket og retningslinjene rundt sletting.	Følger lovpålagte regler og retningslinjer, men det gjennomføres i stor grad arkivering av personopplysninger fremfor sletting.
Tilgang/Tilgangsstyring	Ca. 400 administrativt ansatte ved NTNU har tilgang til FS.	Rollebasert tilgangsstyring på applikasjonsnivå basert på saksgang.	Rolle- og tilhøringhetsbasert.
-> Logging og kontroll	Lite eller ingen, da tilgangen er begrenset.	I stor grad, både logging og kontroll. Kan tildele begrense kontroll gjennom tilgangsstyring.	Logging og kontroll gjennomføres i stor grad.
Skytjenester (Cloud)	* NA	Spennende utfordring for fremtiden, evt. for saksbehandling. Ikke aktuelt for personopplysninger.	Ikke for personopplysninger.
Tjeneste-orientert Arkitektur	* NA	Kan være en påvirkende faktor for økt personvern, men ikke direkte og alene.	Kan begrense tilgangen til opplysninger gjennom strenge tjenester (spørringer og grensesnitt).
Felles register	Benytter informasjon fra SO, DSF og rapporterer til Lånekassen.	Vil være fordelaktig i fremtiden, men vil gi tekniske og sikkerhetsmessige utfordringer.	Felles register bygget med nærhet til bruksområdet, og som kun inneholder opplysninger som er felles for dem som skal benytte det.

Tabell 5.1: Overordnet oppsummering av dybdeintervju basert på sektor.

* Tema ble ikke tatt opp gjennom dybdeintervjuet.

Del IV

Avslutning

6 Diskusjon

Kapittelet diskuterer viktige aspekter rundt arbeidet som er gjennomført og resultatet av det. Det er vel så viktig å være kritisk til utførelsen av arbeid, som til resultatet av det. Enkelte konsepter og deler av resultatet vil også bli knyttet mot teorien presentert tidligere i oppgaven.

Studiet ble gjennomført for å finne ut hvorvidt det finnes et felles register for personopplysninger, samt om innføring av en ny arkitektur, IdMegler, ville øke personvernet til den enkelte og kvaliteten på lagrede personopplysninger. Det ble i løpet av studiet klart at det er mange avgjørende faktorer og samfunnsutfordringer for å kunne oppnå høy grad av personvern.

Det er tidligere gjennomført lite forskning på området rundt innføringen av ny personvernsarkitektur, da IdMegler foreslås som en helt ny løsning. Samtidig er det gjort evalueringer av dagens løsninger og sett på alternative løsninger for å forbedre personvernet. Dette vil benyttes som sammenlings grunnlag i diskusjonen.

6.1 Personvern og personopplysninger

Personvern og personopplysninger er blitt studert og brukt i stor grad gjennom studiet og oppgaven. Basert på forskningsmetodene kan det si noe om lovverket rundt, dagens praksis og fremtidig bruk av personopplysninger og fokus på personvern.

6.1.1 Definisjonen av personopplysninger

Personopplysninger er definert i gjennom Litteraturstudie og i Personopplysningsloven § 2 ledd en som;

> *Opplysninger og vurderinger som kan knyttes til en enkeltperson*[92].

Det er ikke bare opplysninger om en bestemt person som regnes som personopplysninger, men også opplysninger som knyttet til en person. Eksempler på slike opplysninger er kontonummer og bilnummer. Definisjonen av personopplysninger kommer også klart frem i dybdeintervjuene. Som vi kan lese utifra definisjonen av personopplysninger, gis det rom for tolkning og det har dermed vært avgjørende for oppgaven å avgrense begrepet.

I forbindelse med en videreutvikling av IdMegler, vil det være viktig å definerer personopplysninger og videre hvordan man kan unngå at identifikatoren bryter med anonymiteten til en person.

6.1.2 Holdninger og kjennskap til personvern

Datatilsynet skriver i rapporten *Personvern, tilstand og trender*[93] at folk aldri før har vært så opptatt av hvordan de forvalter sin personlige informasjon som i dag og at personvern er noe alle

[92] Lovdata, LOV 2000-04-14 nr 31: Lov om behandling av personopplysninger (personopplysningsloven), www.lovdata.no, http://www.lovdata.no/all/hl-20000414-031.html, 14.04.2000 ,17.03.2013

[93] Datatilsynet, Personvern: tilstand og trender, www.datatilsynet.no, http://www.datatilsynet.no/Global/04_veiledere/personvernrapport_xx.01.2013, 24.04.2013

kjenner på kroppen. Hele 80 % av Norges befolkning er medlem av et sosialt medium. Sosiale medier har økt spredningen av personopplysninger og satt økt lys på personvern, men ikke bevistgjøringen. Dermed vil det være viktig å ha høyt fokus på innebygget personvern i fremtiden, for å legge til rette for at det ikke gjøres lovbrudd, enten om det tilsiktet eller ikke. Lav kunnskap må forbygges på alternative måter.

I 2004 skrev Teknologirådet i sin rapport, *Holdninger til Personvern*[94], at de unge beskymret seg mindre i forhold til personvernskonsekvenser ved bruk av IT, og svært få trodde personopplysninger om dem var blitt misbrukt. Alder er fremdeles en avgjørende faktor i forhold til kunnskapsnivå innenfor personvern, Spørreundersøkelsen blandt studenter på NTNU viser at de yngste studentene har minst kjennskap til Personvern og Personopplysningsloven, men at personvern er viktig for dem personlig.

Basert på spørreundersøkelsen blant studenter på NTNU, viser det seg at det er lite og manglende kunnskap rundt personvern. 65,8% av respondatene har svart at personvern er viktig eller veldig viktig for dem personlig, mens hele 57,4% svarer at de har liten eller veldig liten kjennskap til Personopplysningsloven. I tillegg har kun 16 % av de spurte studentene bedt om innsyn i personopplysninger om seg selv. I fremtiden vil det være vanskelig å oppdage og registrere brudd på personvernet når de det gjelder, ikke har oversikt over egne personopplysninger og hvilke rettigheter som gjelder. Dette kan bli (er) en samfunnsmessig utfordring i fremtiden.

6.1.3 Lagring/Sletting av personopplysninger (FS2)

Sletting av personopplysninger er vagt definert i Personopplysningsloven og Datatilsynets retningslinjer[95], og styres dermed av lovene definert for lagring av Personopplysninger. Hvor lenge personopplysningene skal lagres avhenger hovedsaklig av personopplysningenes art.

- Personopplysningsloven § 28; *Den behandlingsansvarlige skal ikke lagre personopplysninger lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen. Hvis ikke personopplysningene deretter skal oppbevares i henhold til arkivloven eller annen lovgivning, skal de slettes*[96].

- Datalagringsdirektivet (DLD); *Direktivet krever at medlemslandene må sikre at tilbydere av offentlige elektroniske kommunikasjonsnett og -tjenester må lagre de ovennevnte data*[97] *i minimum seks måneder og maksimum to år*[98].

[94] Teknologirådet, Holdninger til personvern, www.teknologiradet.no, http://www.teknologiradet.no/Rapport_fokusgrupper_9-5lz.pdf.file, 19.09.2005, 24.04.2013

[95] Datatilsynet, Personvern på 1-2-3, www.datatilsynet.no, http://www.datatilsynet.no/personvern/, ukjent, 24.04.2013

[96] Lovdata, LOV 2000-04-14 nr 31: Lov om behandling av personopplysninger (personopplysningsloven), www.lovdata.no, http://www.lovdata.no/all/hl-20000414-031.html, 14.04.2000 , 21.04.2013

[97] * *Data som er nødvendig for å spore og identifisere kilder til kommunikasjon, data nødvendig for å spore og identifisere destinasjon, data nødvendig for å identifisere dato, tid og varighet for kommunikasjonen, data nødvendig for å identifisere type kommunikasjon, data nødvendig for å identifisere brukers kommunikasjonsutstyr og data nødvendig for å identifisere lokalisering av mobilt utstyr. Også data knyttet til mislykket oppringning skal lagres (unsuccessful call attempt).* Kilde: http://europalov.no/rettsakt/datalagringsdirektivet-lagring-av-data-fra-elektronisk-kommunikasjon/id-309

[98] Regjeringen, Datalagringsdirektivet: lagring av data fra elektronisk kommunikasjon, www.europalov.no, http://europalov.no/rettsakt/datalagringsdirektivet-lagring-av-data-fra-elektronisk-kommunikasjon/id-309, 26.10.2012, 21.04.2012.

- Regnskapsloven § 2.7 andre ledd sa frem til 19. november 2004, at oppbevaringstiden for regnskapsmaterialet var ti år og at dokumentasjon etter dette kunne overføres fra papir til annet medium, forutsatt at originale dokumenter ble oppbevart i 3 år og seks måneder etter regnskapsårets utløp[99]. Etter dette overtok Bokføringslovens § 13; *Regnskapsmateriale som nevnt i første ledd nr. 1 til 4 skal oppbevares i Norge i ti år etter regnskapsårets slutt. Regnskapsmateriale som nevnt i første ledd nr. 5 til 8 skal oppbevares i Norge i tre år og seks måneder etter regnskapsårets slutt*[100].

- For opplysninger av historisk art og verdi gjelder Arkivloven. *I Arkivloven § 9 bokstav c er det gitt bestemmelser om at arkivmateriale ikke kan kasseres* (red.adm slettes) *med mindre det skjer med hjemmel i forskrifter eller etter særskilt samtykke fra Riksarkivaren*[101].

I tillegg kommer det unntak til lovgivingen som påvirker både sletting og lagring av personopplysninger innenfor bestemte bransjer. Personopplysninger kan lagres for historiske, statistiske eller vitenskaplige formål, dersom det kan begrunnes gjennom samfunnsinteresse, men det krever at opplysningene er anonymisert.

I praksis slettes det veldig lite personopplysninger fra systemene i norske virksomheter. Bakgrunnen er den vage lovgivingen, med mange lover og unntak fra lovverket. I samspill med lave lagringskostnader, utgjør dette hovedårsaken til den manglende slettingen av personopplysninger. I de fleste tilfellene trekkes personopplysningene ut fra fagsystemene, anonymiseres, og lagres i arkiver, noe som gjør dem mindre tilgjengelig (Ref. Dybdeintervju).

Personopplysninger er ikke bare et spørsmål om personvern for virksomhetene, men også forretning. Det vil si at det økonomiske aspektet er viktig for virksomhetene, og mye av den innsamlede informasjonen kan anonymiseres og benyttes til markedsundersøkelser o.l.

6.1.4 Eierskap til personopplysninger (FS4)

Eierskap til personopplysninger er et omdiskutert tema, og det er stor uenighet blant de intervjude virksomhetene. Det er også et stort sprik mellom lovverket og dagens praksis. Personopplysningsloven § 8 sier at *Personopplysninger (jf. § 2 nr. 1) kan bare behandles dersom den registrerte har samtykket, eller det er fastsatt i lov at det er adgang til slik behandling.* Personen opplysningene omhandler har bestemte rettigheter knyttet til disse, og det settes krav til databehandler av personopplysninger. Samtidig kan ikke innsamlede personopplysninger, lagret i en virksomhets database, ses på som virksomhetens eiendeler, men informasjon samlet inn ved samtykke til bruk ved bestemte forhold[102].

Fra et eierskapsprespektiv kan man definere personopplysninger som en eiendel,

[99] Regjeringen; Finansdepartementet, Om lov om bokføring (bokføringsloven), www.regjeringen.no, http://www.regjeringen.no/nb/dep/fin/dok/regpubl/otprp/20032004/otprp-nr-46-2003-2004-/12.html?id=128819, xx.11.2004, 22.04.2013.

[100] Lovdata, LOV 2004-11-19 nr 73: Lov om bokføring (bokføringsloven), www.lovdata.no, http://www.lovdata.no/all/hl-20041119-073.html#13, 01.01.2013 , 22.04.2013

[101] Arkivverket; Riksarkivet og statsarkivene, Noark 5-standarden, www.arkivverket.no, http://arkivverket.no/arkivverket/Offentleg-forvalting/Noark/Noark-5/Standarden, 15.03.2013, 22.04.2013

[102] Norsk senter for informasjonssikring: Aanensen, Bruk og misbruk av personopplysninger, www.idtyveri.no, http://www.idtyveri.info/index.php?option=com_content&view=article&id=39:bruk-og-misbruk-av-personopplysninger&catid=8:beskytt-personopplysninger&Itemid=12, ukjent, 21.04.2012

> *Et eiendomsperspektiv på personopplysninger har imidlertid fått ny aktualitet, først og fremst i forhold til bruk av informasjonsteknologi, fordi personopplysninger i større grad har fått økonomisk verdi og kan byttes bort mot varer og tjenester* (Schartum, 2004).

Ved å definere personopplysninger som en eiendom garanterer man for at produktet (eieren av personopplysningene) er garantert utbytte for salget av opplysningene. I tillegg vil det redusere bruk av personopplysninger, da dette vil medføre kostnader for virksomheten som benytter seg av dem. Samtidig vil det være vanskelig å anse personopplysninger som en privat eiendom da det offentlige har legitime krav på personopplysninger, samt grunner for å overføre eiendomsretten til personopplysninger[103].

Dagens praksis er at virksomhetene *eier* opplysningene samlet inn da de forvaltes og vedlikeholdes av dem, men at personen opplysningene omhandler har rettigheter knyttet til opplysningene. Dette er i mange tilfeller samtykket til, men ikke alle har nok kunnskap og kjennskap til tema at de er klar over bruk av egne opplysninger.

6.1.5 Et overordnet personopplysningsregister: Folkeregisteret (FS3)

Gjennom intervjuene med Datatilsynet og Skatteetaten, viser det seg at Folkeregisteret ikke kan benyttes som et overordnet register til personopplysninger slik det er i dag. Det er mangelfullt i forhold til utenlandske statsborgere bosatt i Norge. I tillegg er det for lite fokus på kildene til registeret. Samtidig viser dybdeintervjuene at et overordnet register for personopplysninger vil være fordelaktig i fremtiden. I tillegg er det viktig å ha fokus på bruk og nærhet til bruk ved utvikling av nye registre. Dette vil medføre høyere kvalitet på innholdet i registeret.

Et overordnet personopplysningsregister vil i fremtiden være fordelaktig fordi det kan senke vedlikeholdskostnadene og øke kvaliteten på lagrede personopplysninger. Samtidig kan det knyttes store utfordringer til et overordnet register. Både sikkerhetsmessig, i forbindelse med oppetid og tilgangsstyring, for å nevne noen eksempler. I tillegg vil kildene til registeret være avgjørende for kvaliteten til innholdet og personopplysningene lagret i registeret. Her kan nærhet til bruk av registeret og personopplysningene lagret i registeret gi økt kvalitet.

Det finnes i dag eksempler på bransjer hvor det er utviklet normer og retningslinjer for behandling og utvikling av personvernslovlige systemer, samt etterlevelse av disse og krav for oppfølging. NOD, nasjonal ordredatabase (Datatilsynet: Bransjenorm, 2010), er utviklet i samarbeid med de ulike aktørene i kollektivtransportbransjen og tanken er at den i fremtiden vil kunne benyttes på landsbasis.

For å kunne benytte et overordnet register, i samspill med IdMeger-arkitektur, argumenter Datatilsynet for at registeret må være offentlig, mens både virksomheten og drifteren av megleren kan være private. Resultatet fra spørreundersøkelsene viser at studentene med teknologisk bakgrunn

[103]Regjeringen; FAD, NOU 2009: 1, Individ og integritet, www.regjeringen.no, http://www.regjeringen.no/nb/dep/fad/dok/nouer/2009/nou-2009-1/5/2/1.html?id=542082, ukjent, 19.03.2013

ønsker seg et privat register, mens studenter med samfunnsvitenskaplig bakgrunn vil ha et offentlig register.

6.1.6 Tjeneste-orientert arkitektur (FS1)

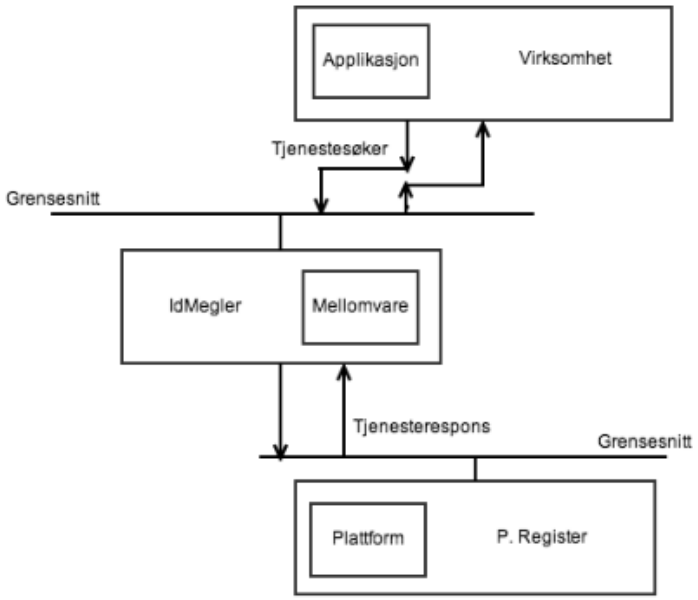
Tjeneste-orientert ariktektur ble presentert gjennom litteraturstudie og er definert som en samling av tjenester som kommuniserer med hverandre ved hjelp av enkel sending av data (Barry, 2002), se kapittel 2.4.6. Hovedfordelen med arkitekturen er muligheten for å skjerme tjenestesøkende fra endringene i tjenestene, som også er en av tankene bak IdMegler. Tjeneste-orientert arkitektur og IdMegler kan ses i samspill med mellomvare-tjenester. En mellomvaretjeneste er en generell tjeneste eller et programlag som befinner seg mellom en eller flere plattformer og overliggende applikasjoner (Bernstein, 1996). Mellomvaren leverer tjenester til andre systemer.

Figur 6.1 viser en illustrasjon av sammenhengen mellom prinsippene for tjenesteorientert arkitektur, mellomvaretjenester og IdMelger. Her opptrer IdMegler som en mellomvare-tjeneste mellom plattformen med personregisteret og applikasjonen hos en bestemt virksomhet. Applikasjonen opptrer som tjenestesøker og får en tjenesterespons fra plattformen ved hjelp av mellomvaren. Ved bruk av IdMegler som en tjeneste-orientert arkitektur vil det være viktig å se på aspektene til Standardiseringssekretariatet i rapporten *Anbefalinger til standardiseringsrådet om oppfølging av utredningen om mulige standarder for en tjenesteorientert arkitektur i offentlig sektor*[104];

- Mengden data som skal overføres fra tjenestetilbyder til tjenestesøker.
- Frekvensen på data som skal utveksles mellom tjenestetilbyder og tjenestesøker.
- Formen på dataene, avsender og mottaker teknologi.
- Behovet for sikkerhet.

Punktene avspeiler mange av hovedpunktene som kommer igjen gjennom intervjuene, som utfordringer, men også som store forbedringsområder for fremtiden. Både for økt sikkerhet, kvalitet og personvern.

[104]Difi; Standardiseringssekretariatet, www.standard.difi.no, Anbefalinger til standardiseringsrådet om oppfølging av utredningen om mulige standarder for en tjenesteorientert arkitektur i offentlig sektor, 08.03.2010, 22.04.2013.



Figur 6.1: Illustrasjon av IdMelger ved bruk av mellomvare og tjeneste-orientert arkitektur

Gjennom intervjuene er det stor enighet om at en tjeneste-orientert arkitektur ikke direkte kan forbedre anonymiseringen av personopplysninger i forhold til Personopplysningsloven. Det argumenteres for at en tjeneste-orientert arkitektur kan øke personvernet ved at virksomhetene lagrer og tilbyr egne tjenester, og ikke sender kopier av data/registre til andre virksomheter som forvalter og behandler data for dem. Da har virksomheten som oppbevarer registeret, mulighet til å benytte logging og se hvem som har gjort hva i ettertid - kontroll. Samtidig oppnår man høyere grad av personvern ved å skille ut personopplysninger fra fagsystemene i den grad transaksjonene og saksbehandlingsdata vil anonymiseres. I tillegg kan arkitekturen øke kvaliteten på lagret data, samt mulighetene for å distribuere løsninger og ikke datasett.

Noen ganger vil det være hensiktsmessig å duplisere data og registre. I noen tilfeller blir systemkravene for høye til at virksomhetene klarer å behandle dem selv, Larsen, Datatilsynet.

Wesenberg argumenterte for at en tjeneste-orientert arkitektur øker personvernet gjennom begrensning av tilgang til opplysninger laget i databasen/plattformen. Gjennom grensesnittet kan det settes retningslinjer og det muliggjøres bestemte spørringer som igjen kan skjule ulike innsynsvinkler for brukerne av systemet.

6.1.7 Identitetstyveri

Veldig mange har vanskelig for å skille identitetstyveri og personvern. Identitetstyveri er i hovedsak bruk av en annen persons identitet ved å skaffe seg tilgang til og ressurser eller rettigheter som tilhører en annen (Hornnes, 2009). Det vil si misbruk av andres personopplysninger gjennom et ønske om å påføre noen andre skade eller ubehageligheter. I rapporten er det evaluert og sett på muligheten for at en ny personvernsarkitektur kan være en bidragsyter til å bekjempe identitetstyveri.

Identitetstyveri kan ses i sammenheng med datakriminalitet. For å begrense det stadig økende problemet datakriminalitet, oppstod begrepet PET (Privacy-enhancing technologies), en kobling mellom teknologi og personvern (Regjeringen, Personvernøkende teknologi og identitetsforvaltning, 2009). Hovedformålet ved PET er å tilrettelegge for overholdelse av lovverket og retningslinjene knyttet til Personopplysningsloven, samt øke kvaliteten på lagret personinformasjon.

> *Fokuset på identitet kan forklares ved at personverninteresser ikke gjør seg gjeldene dersom opplysningene gjelder ikke kan identifiseres* (Regjeringen, Personvernøkende teknologi og identitetsforvaltning, 2009).

Ved å skille mellom identitet og personvernsinteresser vil det forsterke den enkeltes personvern. Basert på dette, kan vi si at identitetstyveri ikke er personvern, men kan ses som et relatert begrep, da de i stor grad kan påvirke hverandre.

6.1.8 Synet på personvern, egne holdning og kjennskap

Gjennom studiet har jeg fått en bred innsikt i personvernsregler og -lover, samt i forholdet mellom personopplysninger, personvern og teknologi/arkitektur. Da jeg startet arbeidet med studiet hadde jeg personlig liten eller middels kjennskap til personvern. Personlig var mitt forhold til personvern knyttet til sosiale medier, Google, Apple og lange utledninger som måtte godkjennes for å bekrefte kjøp og opprettelse av profiler. I løpet av studiet har jeg fått en bedre innsikt og forståelse for mine egne rettigheter og hva jeg kan forvente av virksomheter som lagrer opplysninger om meg.

Til tross for at jeg har fått et bedre innsyn i hvor lett personopplysninger kan kobles og dermed misbrukes, har ikke forholdet mitt til personvern endret seg i stor grad. Samtidig har jeg blitt mer bevisst, og mer bestemt på hvilke opplysninger jeg ønsker å dele, og hva jeg ikke ønsker å dele.

6.2 Vurdering av datagrunnlag

Dette kapittelet tar for seg en vurdering av datamaterialet i studie, og om det kvalitetsmessig kan trekkes en god konklusjon basert på det. De to vanligste målene for datakvaliet er reliabilitet og validitet.

6.2.1 Reliabilitet

Reliabilitet henspeiler hvorvidt datamaterialet i studie er pålitelig (Grønmo, 2004). Datamaterialet vil avgjøre kvaliteten på de analytiske konklusjonene som blir trukket gjennom studiet, og det er derfor avgjørende at datamaterialet er pålitelig.

Det argumenteres for at reliabiliteten i en studie er høy dersom tilsvarende forskning oppnår samme resultat. Samtidig vil det knyttes samfunnsmessige utfordringer til dette. Grønmo argumenterer for at mange av fenomenene som studeres er komplekse og i stadig endring, og fordi forskningsmetodene er lite standardiserte, vil det være vanskelig å gjennomføre like studier. Videre er det viktig å

ta hensyn til forskningsmetodene benyttet gjennom studiet, og fleksibiliteten i disse. Kvalitative metoder kan vanskeliggjøre replikasjon av studiet.

Studiets tre forskningsmetoder er litteraturstudie, intervju og spørreundersøkelse, alle kjente og velbrukte metoder i ulike fagmiljø. Intervjuguidene og spørreundersøkelsene benyttet gjennom innsamlingsprosessen vil være tilgjengelig for fremtidige studier. Videre ivaretas reliabiliteten i studiet ved referanselisten, en oversikt over ulike rapporter, faglige bøker, tidligere studier og offentlige dokumenter, antakelser og avgjørelser studiet baseres på. Basert på dette og forutsatt at de samme personene og virksomhetene ble intervjuet, vil jeg si at studiet kunne vært gjennomført på nytt med tilsvarende resultatet. Dette baserer seg også på at samme målgruppe ble inkludert i forbindelse med besvarelse av spørreundersøkelsene.

6.2.2 Validitet

Studiets validitet handler om produktet og resultatets (problemstillingens) gyldighet. Validitet er et mål på om datainnsamlingen undersøker det den skal undersøke. Den vil være høy dersom datainnsamlingen fremskaffer data som har relevans for problemstillingen (Grønmo, 2004). Validitet kan deles i to, intern og ekstern validitet. *Intern validitet* handler om i hvilken grad resultatene er gyldig for det utvalget og fenomenet som er undersøkt. *Ekstern validitet* er i hvilken grad resultatene kan overføres til andre utvalg og situasjoner.

Grønmo argumenterer for at validitetsbegrepet kan deles inn i ytterligere tre komponenter;

- *Kompetansevaliditet* viser til forskerens kompetanse i forbinnelse med datainnsamling innenfor det aktuelle kompetanseområdet (Studiens interne validitet).
- *Kommunikativ validitet* er samtaler mellom forsker og andre for å avgjøre hvorvidt datamaterialet belyser den aktuelle problemstillingen.
- *Pragmatisk validitet* er i hvilken grad studien tilrettelegger for handlinger (Studiens eksterne validitet).

Kompetansevaliditeten kan påvirke studien med bakgrunn i forskers akademiske nivå som mastergradsstudent. Forskers kompentanse begrenser seg til faglige emner på universitetet, kurs og konferanser, samt bacheloroppgave, men ikke arbeid i lignende størrelsesorden. Mangel på erfaring trenger ikke påvirke studien i stor grad da veiledning er gjennomført av fagpersoner med høy kompentanse og lang erfaring innenfor fagområdet, i tillegg til mange innspill fra fagpersoner innenfor personvernsområdet.

Kommunikativ validitet er opprettholdt gjennom hele studiet ved kontinuerlige samtaler med vitenskaplig ansatte på instituttet (IDI), hos NTNU IT, medstudenter, og fagpersoner i offentlige og private virksomheter. Validiteten kan svekkes basert på personlige synspunkt ved vurdering av datamaterialet, men utstrakt diskusjon med ulike aktører vil redusere faren for dette.

Pragmatisk validitet handler om studiets eksterne validitet, og tilrettelegging for handling basert på resultene oppnåd gjennom studiet. Høy pragmatisk validitet oppnås dersom studie i etterkant fører til endringer. Studiet har bidratt til økt bevisst- og synliggjøring av rettigheter knyttet til personvern, samt en tilretteleggelse for å unngå lovbrudd, med eller uten hensikt. Dermed tilrettelegger studiet for økt informasjon, og dermed også til mer opplysninger og synliggjøring av tema.

6.2.3 Valg av metode

Gjennom oppgaven og studie er det benytte tre ulike metoder, litteraturstudie, spørreundersøkelser og dybdeintervju, som til sammen danner forskningsmetoden. Ved bruk av flere ulike metoder vil resultatet gi et bedre bilde av virkeligheten og fremtidige muligheter. Bruk av en isolert metode kan gi et feilaktig inntrykk og ingen konklusjoner blir trukket basert på det.

Dybdeintervju og kvalitative data kan være vanskelig å analysere, og kan bære preg av intervjuobjektets egne meninger og tanker. Disse vil ikke nødvendigvis være objektive. Dybdeintervjuene ble gjennomført etter semistrukturerte intervjuguider. I noen tilfeller ble ikke hele intervjuguiden gjennomgått, fordi avsporingene og diskusjonene ga mer verdifull og relevant informasjon for oppgaven. I tillegg ga de ulike rollene og akademiske bakgrunnene til intervjuobjektene ulik grad av kompetanse og kunnskap rundt alle tema. I etterkant ble intervjuene transkribert og sendt til intervjuobjektet for tilbakemelding. Etter tilbakemeldingene ble nødvendige endringer gjennomført. Ved bruk av tilbakemelding økte kvaliteten på informasjonen i interjvuene, samt muligheten for å ta bort misforståelser, feil og mangler.

I et av intervjuene fikk jeg følelsen av at intervjuobjektet var forstyrret av Hawthorne-effekten (Intervjuobjekt fikk påvirket atferd av forskerens tilstedeværelse) (Oates, 2006), og redd for at sensitiv informasjon om virksomheten skulle komme på avveie. Dette var ikke et stort problem, men kan til en viss grad ha påvirket resultatet, til tross for at intervjuobjektene har fått mulighet til å avgjøre hvilke opplysninger som kunne benyttes i studiet.

Spørreundersøkelsene og kvantitative data er konkrete og lett å analysere ved hjelp av statistikk. Spørreundersøkelsen rettet mot NTNU studenter hadde et tilstrekkelig antall studenter, men det er vanskelig å være hundre prosent sikker på at det kun er NTNU studenter som har besvart undersøkelsen. Spørreundersøkelsen ble distribuert på NTNU sitt intranett og via sosiale medier. I tillegg er utvalget av respondanter til dels uniformt og kan dermed påvirke inntrykket, men samtidig kan utvalget regnes som representativt i forhold til totalt antall, alder-, kjønn- og studieretningsfordeling. For spørreundersøkelsen rettet mot ansatte i IT-virksomheter, er antallet besvarelser lavt og målgruppen tilnærmet uniform, men undersøkelsen ble utviklet for å støtte opp under resultatene funnet i *Spørreundersøkelse mot studenter på NTNU*.

I forbindelse med spørreundersøkelsen rettet mot studenter på NTNU fikk jeg tilsendt et par tilbakemeldinger fra respondenter på undersøkelsen. Disse gikk hovedsaklig på at muligheten for å besvare et spørsmål nøytralt var utelukket. Dette var ikke et alternativ og avgjort på forhånd at ikke skulle være et alternativ, da enten respondaten var nøytralt enig, eller nøytralt uenig, for å få klarere resultater. Videre ble det også stilt spørsmål med noen av begrepene, og videre om disse burde vært definert i undersøkelsen. Dette er nok en forbedring som kunne vært gjennomført, *personidentitet, personopplysninger* og *personinformasjon* er tildels overlappende begreper og det kan være vanskelig for besvareren å skille disse fra hverandre. Dette kan ha påvirket respondantenes evne til å besvare spørsmålene.

6.2.4 Oppsummering

Oppsummert er reliabilitet og validitet i studien ivaretatt. Det er benytte ulike forskningsmetoder og ulike former for datakilder, samt innspill fra erfarne fagpersoner med høy kompetanse innenfor

fagområdet. Til slutt kan det stilles spørsmål ved om fremgangsmåten for å besvare problemstillingen er god nok?

Basert på valg av kilder, metoder, dokumentasjon av fremgangsmåte og datamaterialet som er benyttet i studiet mener jeg at validiteten og reliabiliteten er tilfredstillende.

6.3 IdMegler

Gjennom studiet har en av hovedoppgavene vært å undersøke en personvernfremmende og ny arkitekturløsning, IdMegler, samt muligheten og behovet for innføringen av en personvernsinfrastruktur, -system og -tjeneste.

IdMegler kan helt overordnet beskrives som et mellomvaresystem med roller og kan dermed opptre som et nøkkelregister for mapping mellom nøkler, og igjen fremstå som en indeks mellom to systemer. IdMegler skal etableres for å gjøre identitetsmeling mellom en overordnet kilde for personopplysninger og saksbehandling relatert til personen. Dermed vil hovedoppgaven være sammenkobling av saksbehandlingsdata og personopplysninger.

Som skrevet i kapittelet om IdMegler, 2.5, skal IdMegler opptre som en megler mellom et personregister og de som ønsker å bruke personopplysningene, på en slik måte at det verken er direkte sporbarhet mellom benyttede nøkler hos en bruker eller at personregisteret har slike koblinger mellom bruk og opplysninger. Brukskonteksten eksisterer så lenge det er kontakt mellom bruker, virksomhet, IdMelger og personregister. IdMegler gir ingen direkte adgang til personregisteret eller til saksbehandlingsdata på personen, siden disse ikke finnes i IdMegler. Videre logger IdMegler bruk av personopplysninger, enten på virksomhets-, prosess- eller transaksjonsnivå. Loggene gir ikke mulighet til å finne ut hvor mange personer en virksomhet har tilknytning til, det kan løses ved bruk av sertifikater og bedriftsregistre. Slike koblinger kan også benytte IdMegler for å hindre direkte sporbarhet. Det finnes også en innsynstjeneste gjennom IdMegler, denne må ikke nødvendigvis implementeres, men vil opptre som en bruker på lik linje med andre tjenester. Den største forskjellen er at brukeren selv initierer og blir autentisert gjennom MinId, BankId eller lignende.

Et annet viktig fokus vil være å ta for seg løsningene på mottakersiden, hvordan applikasjonene vil behandle personopplysningene som blir tilsendt fra personregisteret/databasen. Mottakersiden har vanligvis en allerede eksisterende arkitektur det integreres mot, dermed vil det være ulike tilfeller, og dermed også ulike løsninger. Hovedfokuset i en godt implementert løsning vil være en helhet med sammenkobling av de ulike rollenes aktivitet og et klart uavhenig skille mellom dem (Difi: Tjenesteorientert arkitektur, 2010).

Basert på undersøkelser og intervjuer viser det seg at en løsning som IdMelger, i samspill med et overordnet personopplysningsregister vil gi fordeler i fremtiden. Et stort personopplysningsregister kan være fordeltaktig på tvers av bransjer og virksomheter, men en løsning som IdMegler kan gi sikkerhetsmessige- og tekniske utfordringer. Et overordnet register med personopplysninger vil være spesielt sårbart for sikkerhetshull og det vil settes store krav til autentisering, operabilitet og interoperabilitet.

6.3.1 Sårbarhet

I et av intervjuene ble det argumentert for at koblingene mellom personregisteret og IdMegler, samt mellom virksomhet og IdMegler ville være sårbart for sikkerhetsbrudd.

IdMelger har ingen åpenbare risikoer, men bortfall av tjenesten kan medføre utfordringer. Det vil si dersom koblingene blir brutt uventet, eller dersom koblingene ikke blir opprettet. Dersom det ikke er mulig å få tilgang til personopplysningene kan det skape store problemer for saksgang og -flyt i systemene. Utfordringene vil da være å finne en løsning som ikke krever kobling, og eventuelt benytte seg av lokale registre.

6.3.2 Utfordringer

Baar Larsen uttalte i forbindelse med intervju hos Datatilsynet at;

> *- Helt konseptuelt: tilgangstyring i store registre er vanskelig, om nesten ikke umulig!*

Ved utvikling av IdMegler-arkitekturen viser det seg gjennom dybdeintervjuene at det vil være utfordinger knyttet til skalerbarhet, og det å benytte et stort personregister. I tillegg vil det være utfordringer knyttet til det å sette fokus på kildene til personregisteret, samt opprettholde kvaliteten på lagrede opplysninger. Gjennom intervjuene ble det argumentert for at nærhet til personregisteret gir et høyere kvalitetsmessig innhold, samt at det i mange tilfeller ville være fordelaktig å tilpasse registeret til bruk.

Det vil være utfordringer knyttet til sikkerhet, oppetid, operabilitet, tilgjengelighet, kompleksitet, og tilgangsstyring. Det vil være viktig å ha høyt fokus på kildene til registeret og kvaliteten på opplysningene lagret i personregisteret. Dette blir en mer omfattende prosesser etterhvert som størrelsen på personregisteret øker. Dette vil ikke være en indirekte utfordring knyttet til IdMegler, selv om IdMegler i grunn er en tabell som kan spres over mange noder.

En annen utfordring kan være å opprettholde ytelsen for systemen. Denne kan bli lavere som et resultat av at man ikke benytter meningsbærende nøkler og de derfor må byttes hver gang.

6.3.3 Begrensninger og krav for IdMegler

Ved bruk av Folkeregisteret som personregister kan IdMegler-arkitekturen kun tas bruk dersom både registeret og virksomhetene, som benytter det, er offentlige virksomheter*[105]. Dette er begrunnet gjennom Folkeregisterloven, og det er lovlig gunnlag for deling dersom det finnes paragrafer i enkeltlover som sier at informasjon kan utleveres eller innhentes. Tilgang til Folkeregisteret er sterkt begrenset og tilgang forvaltes og styres av Skatteetaten, basert på innsendte søknader. Offentlige virksomheter kan gis tilgang til opplysninger i Folkeregisteret basert på § 14 i Folkeregisterloven;

[105]* En offentlig virksomhet er et organ som har mulighet til å forbedre og/eller fatte forvaltningsvedtak etter reglene i Forvaltningsloven.

> *Uten hinder av taushetsplikten etter § 13 kan det i medhold av lov eller regler fastsatt av departementet gis opplysninger fra folkeregisteret til offentlige myndigheter til bruk i deres virksomhet.*

Private virksomheter kan få tilgang til ikke-taushetsbelagte opplysninger i Folkeregisteret, så lenge det kan argumenteres for at tilgangen til opplysningene er for å ivareta lovmessige rettigheter. Dette reguleres gjennom Folkeregisterloven § 13;

> *Opplysninger nevnt i første ledd som det ikke gjelder taushetsplikt for, kan utleveres til personer og private institusjoner når opplysningene er nødvendige for å ivareta lovmessige rettigheter eller plikter.*

Lovgivingen viser at deling av informasjon og opplysninger kan skje både med og uten samtykke. Det vil i stor grad være fordelaktig at både virksomheten og registeret er offentlige. Samtidig finnes det et par tilfeller hvor virksomheten er privat, (red.adm Ovenfor private virksomheter er opplysningene i DSF underlagt taushetsrett, begrenset taushetsplikt og taushetsplikt), for eksempel inkasso- eller eiendomsvirksomheter.

Dersom personregisteret er privat, trenger ikke dette være noe problem.

6.4 Resultatene/Samfunnsmessige bidraget

Studiet har hovedsaklig opptredd som et bindeledd mellom personvern og teknologi og har bidratt ved å øke bevist- og synliggjøringen av hver enkelts rettigheter knyttet til personvern, og egne personopplysninger.

Ved bruk av IdMegler vil det tilrettelegges for å unngå lovbrudd, enten med eller uten hensikt, samt redusere faren for utro tjenere. En innføring av ny arkitektur vil også begrense spredningen av personopplysninger, øke kvaliteten på dem som er lagret og redusere konstnadene knyttet til vedlikehold av dem.

7 Konklusjon

Gjennom dette kapittelet gis en konklusjon for forskningsspørsmålene og videre for problemstillingen, basert på arbeidet som er gjort gjennom studien og oppgaven.

7.1 Forskningsspørsmål

For å besvare problemstillingen må først de fire forskningsspørsmålene besvares og konkluderes. Dette gjøres basert på arbeidet gjennomført i studiet.

- *FS1: Hvordan kan en tjeneste-orientert arkitektur forbedre anonymiseringen av personopplysninger i forhold til Personopplysningsloven? og igjen være bidragsyter til å bekjempe identitetstyveri?*

Forskningsspørsmål 1 må deles i to for å kunne besvares. Et brudd på Personopplysningsloven er ikke det samme som et identitetstyveri. Et identitetstyveri er tilsiktet og med hensikt, her utgir vedkommende seg for å ha en identitet han/hun ikke har.

FS1.1 Hvordan kan tjeneste-orientert arkitektur forbedre anonymiseringen av personopplysninger i forhold til Personopplysningsloven?

Tjeneste-orientert arkitektur kan ikke direkte forbedre anonymiseringen av personopplyninger, men være et viktig ledd i prosessen ved at man kan hindre unødvendig duplisering av informasjon på tvers av systemer og at man i mye større grad kan kontrollere adgang til opplysninger gjennom autoriasjon.

FS1.2 Hvordan kan tjeneste-orientert arkitektur være bidragsyter til å bekjempe identitetstyveri?

Tjeneste-orientert arkitektur kan være en bidragsyter, men ikke direkte for identitetstyveri.

- *FS2: Hvilke teknologisk støtte/prosess har du som person i forhold til å hente ut/få innsyn i/slette personopplysninger om deg selv, lagret hos ulike virksomheter på nett?*

Innsyn i personopplysninger og sletting av personopplysninger er to helt forskjellige handlinger og må besvares separert.

Innsyn i personopplysninger lagret hos en virksomhet er lovpålagt i Personopplysningslovens §18. Enhver som ber om det, har rett til innsyn i personopplysninger lagret, men også rundt saksgang og hvordan opplysningene er behandlet. De fleste virksomheter har også retningslinjer og teknologiske hjelpemidler for behandling av innsynsforespørsler.

Sletting av personopplysninger avgjøres utifra regler gjeldene for lagring av personopplysninger. Hvor lenge personopplysninger skal lagres, avgjøres utifra opplysningsens art. Ved sletting av personopplysninger er virksomhetene i stor grad underlagt krav som Personopplysningsloven stiller, samt Datatilsynets retningslinjer.

- *FS3: Er det mulig og hensiktsmessig å opprette en felles kilde til personopplysninger/et felles folkeregister for personopplysninger? Hvor stor del av personopplysningene som lagres i dag er statiske? og igjen hvor mange av dem er knyttet til bruk?*

Forskningsspørsmål 3, er et todelt spørsmål og deles opp for å kunne besvares.

FS3.1 Er det mulig og hensiktsmessig å opprette en felles kilde til personopplysninger/et felles folkeregister for personopplysninger?

Ja, det er hensiktsmessig å opprette et overordnet personopplysningsregister for personopplysninger i fremtiden på fysisk eller logisk nivå. Ja, det vil være mulig å opprette et slik register, men det vil settes høye krav til det, i forbindelse med opptid, tilgangsstyring og behandling.

FS3.2 Hvor stor del av personopplysningene som lagres i dag er statiske? og igjen hvor mange av dem er knyttet til bruk?

Med utgangspunkt i Personopplysningslovens definisjon av personopplysninger kan nesten alle personopplysninger regnes som statiske. Noen av personopplysningene vil endre seg iløpet av et menneskeliv, men dette er i utgangspunktet så få ganger at de kan regnes som statisk. Den mest brukte personopplysningen er i dag personnummeret, som benyttes som personidentifikasjon i mange systemer. Fødselsdato og navn benyttes også i noen tilfeller, men denne kombinasjonen kan ikke tilby en unik identifikator for en person.

- *FS4: Hvem eier informasjonen som er lagret hos en virksomhet om en person?*

Forskningspørsmålet har ikke et klart og definert svar, da det er stor uenighet rundt spørsmålet og et sprik mellom lovverket og dagens praksis. Lovverket sier at personen opplysningene omhandler, eier personopplysningene dersom ikke annet er avklart/samtykket til. Dagens praksis er at virksomhetene eier opplysningene samlet inn da de forvaltes og vedlikeholdes av dem, men at personen opplysningene omhandler har rettigheter knyttet til opplysningene.

7.2 Problemstillingen

Problemstillingen som skulle besvares gjennom oppgaven, ved hjelp av forskningsspørsmålene var, *Det finnes ikke et felles register for personopplysninger.*

Basert på litteraturstudie, dybdeintervju og spørreundersøkelser utført i forbindelse med oppgaven kan det konkluderes med at det ikke finnes et felles register for personopplysninger. Det nærmeste man kommer er DSF, folkeregisteret, men dette vil ikke være tilfredstillende for bruk i forbindelse med IdMegler-arkitekturen.

7.3 IdMegler

Basert på studiet og arbeidet gjennom oppgaven viser det seg at IdMegler som arkitektur er mulig å gjennomføre. Dette kan begrunnes og understøttes gjennom spørreundersøkelsene og dybdeintervjuene med virksomheter i privat og offentlig sektor. Spørreundersøkelsene viser at det er liten

kunnskap rundt personvern og at det i utviklingen av nye systemer vil være viktig å fokusere på innebygget personvern. Gjennom intervjuene kommer det frem at Skatteetaten, Statoil og Sparebank 1-gruppen har systemer (under utvikling) som bygger på de samme prinsippene som IdMegler. I disse løsningen er det fokus på å samle informasjon i et system, videreutvikle tilgangsstyringen til personopplysninger, og til en viss grad skille person- og saksbehandlingsopplysninger. Skatteetaten argumenterer også for at tjeneste-orientert arkitektur kan forbedre anonymiseringen av personopplysninger og bidra til økt personvern, gjennom at virksomhetene selv lagrer og tilbyr tjenester. Figur 6.1 viser hvordan IdMegler kan benyttes som tjenste-orientert arkitektur, med IdMegler som mellomvare.

IdMegler vil gi personvernmessig gevinst både for virksomhetene og berørte personer. IdMegler muliggjør bruk av et overordnet personregister, som vil være fordelaktig i forhold til bruk, kvalitet og konsistens på lagrede personopplysninger og ved vedlikehold. I tillegg vil en løsning som IdMelger redusere antallet dupliseringer av personopplysninger og registre hos virksomhetene. Ved bruk av nøkkelgenerering vil også sikkerheten rundt personopplysningene øke, samt gi muligheter for tilgangsstyring og logging på et høyere nivå. For brukerne vil IdMegler gi brukerne mer kontroll hvor egne personopplysninger. IdMegler gir oversikt over hvem som lager personopplysninger, hvilke personopplysninger som lagres, når personopplysningene blir brukt og hvem som har tilgang til dem. Dette gir brukerne et forhold til egne personopplysninger, og en mulighet for å kontrollere egen informasjon.

Videre kan IdMegler muliggjøre bruk av skytjenester ved at virksomhetene legger saksbehandlingen ut i skyen.

IdMegler har i utgangspunktet ingen åpenbare riski og som konkludert med kan arkitekturen benyttes og medfører økt personvern for den enkelte, ved bestemte forutsetninger.

8 Videre arbeid

I det videre arbeidet bør det ses på ulike teknologier, sikkerhetsmekanismer og implementasjonsmuligheter.

I første omgang bør det utvikles en detaljert teknisk kravspesifikasjon for arkitekturen, både for IdMegler og personregisteret. Det bør også opprettes en forretningsplan for hvordan IdMegler skal utvikles, forvaltes og benyttes. I tillegg kan det være fordelaktig å komme i kontakt med ulike offentlige og private virksomheter som kunne tenkt seg å benytte løsningen. Videre bør det utvikles en pilot-arkitektur for testing og tilslutt implementasjon.

Nøkkelteknologier i den tekniske utviklingen kan være:

- Databaser/registre
- Web Services
- WS Security (autentisering og autorisering)
- Workflow og workflow security
- Rollestyring og autorisasjonsteknologi, en mulig integrasjon med BankId, MinSide eller Alltinn
- Hvordan IdMegler skal integreres som mellomvare
- Elektronisk Id på virksomhet, arbeidsprosess og bruker , samt på person for få tilgang til informasjon knyttet til bruk av IdMegler.

9 Referanser

(Aaserud, 2012) Aasrud R. (2012) *På nett med innbyggerne*. Hentet 15.11.2012 fra: http://www.regjeringen.no/nb/dep/fad/aktuelt/taler_og_artikler/minister/taler-og-artikler-av-fornyings–og-kirke/2012/pa-nett-med-innbyggerne.html?id=678357

(Ackerman, 2004) Ackerman, M. (2004). *Privacy in Pervasive Environments: Next Generation Labeling Protocols*, Personal and Ubiquitous Computing (8:6), pp. 430-439. London UK: Springer-Verlag.

(Barry, 2002) Barry, D. K. (2002), *Service-oriented architecture (SOA) definition*. Hentet 12.11.2012 fra: http://www.service-architecture.com/web-services/articles/service-oriented_architecture_soa_definition.html

(Bernstein, 1996) Bernstein, P. A. (1996). *Middleware: a model for distributed system services. Communications of the ACM*, 39(2): 86 – 98. New York, USA: ACM.

(Bing, 1991) Bing, J. (1991), *Handbook of legal information retrieval.* Oslo, Norge: Norwegian Research Center for Computers an Law.

(Bråten, 2008) Bråten, M. *(2008), - Personvern under press - hvor går grensene i arbeidslivet?* Hentet 12.09.2012 fra: http://www.fafo.no/pub/rapp/20076/20076.pdf

(Czaja, 1996) Czaja, R. og Blair, J. (1996). *Designing surveys : a guide to decisions and procedure*s. Thousand Oaks, California: Pine Forge Press.

(Dalland, 2007) Dalland, O. (2007). *Metode og oppgaveskriving for studenter* 4. utg. Oslo, Norge: Gyldendal akademiske.

(Datatilsynet: Bransjenorm 2010) Datatilsynet (2010), - *Bransjenorm - for personvern og informasjonssikkerhet i elektronisk billettering*. Hentet 04.09.2012 fra: http://www.datatilsynet.no/global/04_veiledere/bransjenormer/bransjenorm_e-billettering_endelig_01.pdf.

(Datatilsynet, 2010) Datatilsynet (2010). *Fortell med hva dere gjør!* Hentet 06.11.2012 fra: http://www.datatilsynet.no/Global/04_analyser_utredninger/2011/30062011_Nettkontroller_2010_-_analyse.pdf

(Difi, 2010) Difi, Direkorrat for forvaltning og IKT (2010). *Nasjonale felleskomponenter i offentlig sektor*. Hentet 06.11.2012 fra: http://www.Difi.no/filearchive/Difi-rapport-2010-17-nasjonale-felleskomponenter-i-offentlig-sektor-pdf-.pdf

(Difi, 2012) Difi, Direkorrat for forvaltning og IKT (2012). *Overordnede IT-arkitekturprinsipper for offentlig sektor, versjon 2.1*. Hentet 06.11.2012 fra: http://www.Difi.no/filearchive/arkitekturprinsipper-2.1.pdf

(Difi: Id-porten, 2012) Difi, Direktorat for forvaltning og IKT (2012). *ID-porten/MinID, Om eID-leverandørene*. Hentet 05.11.2012 fra: http://www.Difi.no/artikkel/2010/10/om-eid-leverandorene

(Difi: Tjenesteorientert arkitektur, 2010) Difi (2010). *Kartlegging av mulige standarder for tjenesteorientert arkitektur i offentlig sektor, Forprosjektrapport*. Hentet 06.11.2012 fra: http://standard.Difi.no/filearchive/forprosjektrapport-mulige-standarder-for-tjenesteorientert-arkitektur.pdf

(Ghauri, 2005) Ghauri, P. og Grønhaug, K. (2005). *Research Methods in Business Studies*. Manchester, UK: Pearson Education Limited.

(Grønmo, 2004) Grønmo, S. (2004). *Samfunnsvitenskapelige metoder*. Bergen: Fagbokforlaget

(Hornnes, 2009) Horrnes, S. (2009). *Elektronisk identitetstyveri*. Masteroppgave ved UIO. Oslo.

(Juul, 2011) Karsten Juul (2011), Nogle emner fra beskrivende Statistik, http://www.mat1.dk/beskrivende_statistik.pdf

(Kobsa,2003) Kobsa, A. (2003): *A Component Architecture for Dynamically Managing Privacy Constraints in Personalized Web-Based Systems,* Berlin, Heidelberg, Tyskland: Springer-Verlag.

(Kvale, 2009) Kvale, S. (2009). *Det kvalitative forskningsintervju*. Gyldendal Norsk Forlag AS.

(Langheinrich, 2002) Langheinrich M. (2002): *A Privacy Awareness System for Ubiquitous Computing Environments*. Institute of Information Systems, ETH Zurich. Berlin Heidelberg: Springer-Verlag

(Lewis, 2009) Lewis D. K. (2009). *Web Single Sign-On Authentication using SAML.* IJCSI Inernational Journal of Computer Science Issues, Vol 2. University of Louisville, KY, USA.

(Li, 2010) Li, X.; Zhou, L.; Shi, Y. & Guo, Y. (2010). *A trusted computing enviroment model in cloud architecture.* Beijing, Kina: Jiaotong University.

(Loshin, 2009) Loshin, D. (2009). *Master data management*. The MK/OMG Press. Morgan Kaufmann.

(Oates, 2006) Oates, B. (2006): *Researching Information Systems and Computing*. London: SAGE Publications.

(Olivier, 2003) Olivier, M. (2003): *A Layered Architecture for Privacy-enhancing Technologies.* Pretoria, Sør Afrika: University of Pretroia.

(Regjeringen: Overtredelsesgebyr, 2008) Regjerningen (2008). *Om lov om endringer i personopplysningsloven mv. (forskriftshjemmel, overtredelsesgebyr og innkreving av tvangsmulkt) - 4. Overtredelsesgebyr*. Hentet 14.09.2012 fra: http://www.regjeringen.no/nb/dep/jd/dok/regpubl/otprp/2007-2008/otprp-nr-71-2007-2008-/4.html?id=519054

(Regjeringen: Personvernøkende teknologi og identitetsforvaltning, 2009) Olsen T. (2009). 1 *Individ og integritet - 4 Personvernøkende teknologi og identitetsforvaltning*. Hentet 13.09.2012 fra: http://www.regjeringen.no/nb/dep/fad/dok/nouer/2009/nou-2009-1/27.html?id=542364

(Rescorla, 2000) Rescorla E. (2000), *SSL and TLS, designing and building secure systems.* LAVOISIER S.A.S.

(Robson, 2002) Robson, C. (2002) *Real World Research; A Resource for Social Scientists and Practitioner- Researchers*, second edition. Blackwell Publishing.

(Sannes, 2005) Sannes, R. (2005), *Dataanalyse og statistikk-kvantitativ tilnærming*, nedlastet kompendiet, http://home.bi.no/fgl88001/metode/index.htm

(Schartum, 2004) Schartum, D. & Bygrave, L. (2004), *Personvern i informasjonssamfunnet.* Fagbokforlaget.

(Schulzrinne, 2008) Schulzrinne, H. (2008), *A Uniform Resource Name (URN) for Emergency and Other Well-Known Services.* IETF. http://tools.ietf.org/html/rfc5031

(Schümann, 2011) Schümann, B. (2011) *Modernisering av folkeregisteret.* Presentasjon fra "Seminar for Statistikkrådet, 12. april 2011": http://www.nokios.no/_media/2011/w3_schurman.pdf

(Smith, 2011) Smith, Dinev & Xu(2011), *INFORMATION PRIVACY RESEARCH: AN INTERDISCIPLINARY REVIEW 1.* MisQuarterly. http://pal.ist.psu.edu/MISQ.pdf

(Solve, 1997) Solve, D. Yale, J. (1997): *Identity Theft, Privacy, and the Architecture of Vulnerability.* Seton Hall Law School.

(Standardiseringsrådet, 2012) Difi, Standardiseringsrådet (2012). *Standarder for en tjenesteorientert arkitektur.* Hentet 06.09.2012 fra: http://standard.Difi.no/filearchive/Standarder%20for%20en%20tjenesteorientert%20arkitektur.pdf

(Stålhane, 2010) Stålhane, T. (2010) *TDT 4235 A short introduction to Quality Assurance for Software.* Tapir akademiske forlag. Trondheim.

(Tanenbaum, 2007) Tanenbaum og Steen(2007): *Distributed Systems: Principles and Paradigms.* Pearson Prentice Hall.

(Thagaard, 2009) Thagaard T., (2009). *Systematikk og innlevelse.* Fagbokforlaget Vigmostad og Bjørke.

(van Blarkom, 2003) van Blarkom, G.W.; Borking, J.J. & Olk, J.G.E. (2003). *"PET". Handbook of Privacy and Privacy-Enhancing Technologies. (The Case of Intelligent Software Agents).* ISBN 90-74087-33-7.

(Årsmelding, 2011) Datatilsynet.no, - *Årsmelding 2011; Tendenser og utviklingstrekk.* Hentet 03.09.2012 fra: http://www.datatilsynet.no/Om-Datatilsynet/Aarsmeldinger/Arsmelding-2011/3-Tendenser-og-utviklingstrekk-/

Del V

Vedlegg

A IdMegler: Prosjektforslag

Oppdragsgiver: Egen

Kontaktperson: Carl-Fredrik Sørensen

Forfatter: Carl-Fredrik Sørensen

Dato: 25.11.2010

Versjon: 0.2

A.1 Bakgrunn

Personvern innenfor databehandling og informasjonsteknologi er tema som opptar mange. Situasjonen i dag er at det finnes mange systemer innenfor enhver virksomhet som holder til dels detaljert informasjon knyttet til personer og bedrifter. En del av denne informasjonen kan være sensitiv eller misbrukes til andre formål enn det som opprinnelig var gitt tillatelse til. Dette fører til en rekke problemstillinger:

- Det finnes ikke en klar autoritativ kilde til personopplysninger. Kildene kan inneholde til dels motstridende informasjon.
- Vedlikehold og lagring av personinformasjon skjer i mange systemer og krever til dels mye ressurser av virksomheter, både persontimer, utstyr, programvare og energi
- Det eksponeres sensitiv informasjon til personer som ikke skal ha eller som ikke har behov for det i sin jobb.
- Det er tilgang til informasjon også når det ikke er tjenestelig årsak til det.
- Mer og mer informasjon blir tilgjengelig over nett med den sikkerhetsrisiko det kan medføre
- Stadig flere bedrifter setter ut drift til eksterne aktører, gjerne utenlands.

Fra ett personvernssynspunkt ønskes det at:

- Hver enkelt person skal kunne vite hvilken informasjon som er registrert om denne.
- Eierskap til en del informasjon hos bedrifter kan i en del tilfeller tilfalle den person informasjon er registrert på og det bør være mulig for personer å begrense eller hindre tilgang til slik informasjon dersom det ikke er ett definert behov for tilgang.
- Personer skal ha tillit til at systemer som inneholder informasjon og transaksjoner knyttet til dem er lagret på en slik måte at informasjonen ikke skal kunne misbrukes eller brukes uten ett klart og lovlig formål.
- Det skal være mulig å fjerne personinformasjon fra aktører som personen ikke lengre har ett (forretnings)forhold ti

A.2 Hovedmål og gevinst

Hovedmålet med konsept og teknologi som blir presentert i dette dokumentet, er å etablere en personvernsinfrastruktur, -system og -tjeneste, heretter kalt IdMegler, med hensikt å:

- Fysisk å splitte mellom (statisk) identifiserende personinformasjon og transaksjoner/annen dynamisk informasjon knyttet til person.
  - Skille ut personregister (kunderegister, personalregister, etc.) på en slik måte at informasjon i slike registre ikke kan benyttes direkte for å finne annen type informasjon knyttet til person.
  - Fjerne direkte identifiserende personkontekst på transaksjoner i databaser og på den måten sikre at ved uautorisert oppslag på transaksjoner så skal det ikke være mulig å koble disse til spesifikke personer.
- Muliggjøre at vedlikehold, kvalitet og sikkerhet knyttet til personinformasjon sikres gjennom bruk av mer autoritative og kvalitetssikrede kilder for denne type informasjon
  - Offentlig personregister kan benyttes som den eneste autoritative kilde for personer
  - Offentlig organisasjonsregister kan benyttes som autoritative kilde for bedriftsinformasjon
  - Redusere antall applikasjoner og databaser som inneholder personinformasjon
- Muliggjøre at en person til enhver tid kan sjekke om hvilke virksomheter som har informasjon knyttet til personen (hvem), hvilken informasjon som er registrert (hva), hvilke formål (prosesser) informasjonen er benyttet i (hvorfor), når informasjon er benyttet.
  - Personer skal kunne benytte offentlig elektronisk identifikasjon som for eksempel MinId gjennom MinSide for autorisering.
- Muliggjøre en kontroll av hvem eller hvilken aktør som benytter personinformasjon og til hvilke prosesser
  - Tilgang til kobling mellom identifiserbar person og informasjon knyttet til denne, må være veldefinert i modellerte og autoriserte arbeidsprosesser, med riktig autorisasjon på virksomhet, arbeidsprosess og saksbehandler
  - Hvert oppslag i personregister logges med hvem (virksomhet/saksbehandler/ ip-adresse/system/systemprosess etc.), hva, når og hvorfor ble det gjort ett oppslag.
    - En slik logg kan benyttes for å kvalitetssikre arbeidsprosesser og samtidig gi mulighet for personer å få innsyn i virksomheters data om personen.
    - Det skal kun gis tilgang til loggen for autoriserte personer i virksomheten, autorisert person som det er registrert tilgang mot, tilsyns-/politimyndigheter ved lovhjemmel
    - Loggen skal beskyttes på samme måte som personinformasjon ved å skille kontekst (person, virksomhet) fra logginnslag.
  - Tilgang til kobling mellom person/arbeidsprosess skal være tidsbegrenset og knyttet til transaksjon startet og avsluttet i arbeidsprosses. Dersom arbeidsprosess ikke er avsluttet innenfor forventet levetid, skal det være mulig å avslutte denne automatisk.

- Sørge for at historiske transaksjoner relatert til personer kan "stenges" dersom det ikke er spesifikke årsaker til at disse skal være synlig.
  - Skille mellom "ferskvare"-informasjon og historisk informasjon, for eksempel knyttet til regnskapsår.
- Det skal ikke være mulig å åpne opp samme kobling flere ganger. Dvs. at nøkler gjort tilgjengelig for kobling mellom transaksjons- og personregistre skal kun benyttes en gang.

IdMegler skal kunne tilfredsstille alle mål som beskrevet ovenfor gjennom etablering av en personvernsinfrastruktur med tilhørende programvare, databaser, algoritmer og tjenester.

IdMegler skal kunne benyttes mot andre type koblinger mellom statisk og dynamisk informasjon, for eksempel i forhold til andre nøkkel/kontekstbærende registre (kunderegister, infrastrukturregister, bygningsregister, våpenregister etc.) og transaksjoner knyttet til disse.

IdMegler skal kunne eksistere både innenfor en virksomhet og som en måte å koble informasjon mellom (private, offentlige) virksomheter.

IdMegler instanser skal kunne knyttes sammen i ett nettverk på en slik måte at det kan etableres en innsynstjeneste for autoriserte enkeltpersoner som ønsker å få tilgang til, og eventuelt gi tillatelse til videre bruk av informasjon for virksomheten.

Logging av bruk av IdMegler skal kunne gjøres på flere nivåer:

- Megling internt i virksomhet
- Megling mellom virksomheter

Viktige sektorer som kan støttes av konseptet er for eksempel informasjonssystemer innenfor helse, skatt, personal, forsvar, forsikring, bank etc.

Både privatpersoner og virksomheter skal kunne bruke IdMegler både for bruk av informasjon og for "godkjennelse" av bruk.

A.3 Strategiske mål som understøttes

Systemet som foreslås vil gjøre virksomheter bedre i stand til å ivareta personvernslovgivning i forhold til hvilke data som registreres for hvilket formål, og hindre at persondata blir benyttet til andre formål enn det som virksomheten har fått tillatelse til.

Personer (og virksomheter) skal kunne benytte systemet ved hjelp av offentlig elektronisk id (for eksempel MinID eller Feide) for innsyn i hvilke data som er registrert om personen og til hvilket formål data er benyttet og lagret.

A.4 Hovedfunksjon

IdMegler (IdBroker/IdMediator) skal etableres for å gjøre identitetsmegling mellom en autoritativ kilde for personinformasjon (for eksempel Folkeregister eller bedriftsintern Personregister) og transaksjonsinformasjon relatert til personen.

Eks. Folkeregisteret inneholder basisinformasjon om personer og kan tilgjengeliggjøre en identifikator (fremmednøkkel – ikke personnummer) som kan benyttes av virksomhetsregister for å identifisere transaksjoner koblet til en spesifikk person. For å få koblet informasjon i virksomhetsregister med folkeregister, må det defineres en arbeidsprosess med autorisasjon både på virksomhet, prosess og på person som utfører den, for å tilgjengeliggjøre IdMegler for å koble sammen intern virksomhetsidentifikator med identifikator som kan benyttes til å finne relevant personinformasjon i Folkeregisteret. IdMegler er ansvarlig for å tilgjengeliggjøre nøkler som kan benyttes i virksomhetens informasjonsregistre for sikre at det er mulighet for en trygg sammenkobling med Folkeregisteret. Alle transaksjoner relatert til person lagres dermed med nøkler tilgjengeliggjort gjennom IdMegler og IdMegler benyttes for å sammenkoble informasjon ved hjelp av nøkkelmegling mellom virksomhet og Folkeregister.

For å sikre at bedrift ikke skal kunne benytte gitt nøkkel til ikke-autoritative aksess utenfor definert arbeidsflyt, kan nøkler relatert til person endres så snart arbeidsprosessen er ferdig. Foreslått system vil kreve at en arbeidsflytmekanisme hos bruker (bedrift) skal kunne sende en notifikasjon til IdMegler når arbeidsflyt er ferdig utført. IdMegler vil da kunne oppdatere nøkkel i transaksjonsregister og hos seg selv slik at informasjon i transaksjonsregisteret ikke kan aksesseres vha samme nøkkel flere ganger. For å hindre at man "låser" informasjon, arbeidsprosess og nøkler, kan det innføres timeout i forhold til forventet tidsbruk, dvs. at IdMegler må kunne sende en timeout til bruker når tidsgrensen er nådd. For å åpne tilgang igjen, må ny nøkkel megles for å få etablert kobling mellom person og informasjon om denne.

Fordel: Transaksjonsinformasjon kan i en del tilfeller frigjøres siden denne informasjonen ikke gir noen mening uten personkontekst, data må derfor ikke nødvendigvis krypteres.

All kommunikasjon mellom bedrift, folkeregister, Idbroker, transaksjonsregister skjer på kryptert kanal. Bruker kan selv få oversikt over hvilke bedrifter som holder informasjon om denne, og kan dersom person har en elektronisk Id, kunne få innsyn i (alle?) data som er registrert om seg. Bedrifter kan få en notifikasjon ved jevne mellomrom om dette. Historiske data kan ikke tilgjengeliggjøres uten spesielt samtykke fra person, eller at bedriften setter i gang spesifikke arbeidsflyter. Person bør få melding når dette skjer.

Adgang til data og personinformasjon må knyttes til spesifikke arbeidsprosesser som en del av ordinær tilgangsstyring i virksomheten. Semantiske nøkler bør unngås så langt som mulig. Nøkler gjøres tilgjengelig på en slik måte at kontekst i arbeidsprosess og autorisasjon styrer hvilke data som skal være tilgjengelig når.

Virksomhet kan benytte eksterne eller interne autoritative personregistre. Disse er fysisk adskilt fra transaksjonsdata. Transaksjonsdata benytter fremmednøkler fra IdMegler slik at all kontekst er fjernet. IdMegler kobler sammen kontekst fra dataeier gjennom autoritativ arbeidsprosess (også kontekst) for å gi tilgang til de transaksjonsdata som det er behov for i prosessen.

Nøkkelteknologier:
Databaser/registre

Web Services
WS Security (autentisering og autorisering)
Workflow og workflow security
Rollestyring og autorisasjonsteknologi
IdMegler mellomvare
Elektronisk Id på virksomhet, arbeidsprosess og bruker
Elektronisk Id på person for å få tilgang til informasjon knyttet til bruk av IdMegler. Tilgang til en slik oversikt kan for eksempel gjøres gjennom MinSide-portalen

Nødvendige forutsetninger:
Informasjon i koblingsregister (IdMegler) kan gjøre uavhengig av både personregister og transaksjonsregister ved å benytte egen teknologi (sette opp en IdMegler mellom to andre IdMeglere)
Autorisasjon lages i forhold til både bruker (kan også være en automatisk prosess), arbeidsprosess og person.
Speiling av IdMegler er nødvendig for å sikre at informasjon ikke forsvinner ved nedetid eller krasj
Bruk av IdMegler er ikke mulig uten riktig autorisasjon, innhold vil ikke ha noen mening siden det ikke registreres hvem som benytter hvilke identifikatorer i kobling.

A.5 Informasjonsinnhold

Basisinformasjon i IdMegler vil være ett nøkkelregister for mapping mellom nøkler. I den enkleste form opptrer IdMegler som en form for indeks for to systemer. IdMegler må kunne inneholde informasjon som gjør logging mulig. Nivå og innhold i logger vil bestemme hvor mye informasjon som det vil være behov for å ta vare på. Loggene bør følge samme konsept for å skille kontekst fra loggtransaksjoner.

Sikkerhet i nøkkelhåndtering (utvidelse av sikkerhet i konseptet): IdNøkler kan genereres basert på krypteringsalgoritmer. Informasjon i IdMegler database kan benyttes for å gi en generert nøkkel til egnet dekrypteringsalgoritme for å kunne gjøre mapping mellom Folkeregister og virksomhet. Transaksjonsregistre kan oppdateres med nye nøkler når informasjon har blitt aksessert.

A.6 Brukerinvolvering

IdMegler vil berøre mange interessenter i forhold til etablering som en tjeneste/teknologi.

- Lovgivere/politikere i forhold til å muliggjøre implementering og etablering av tjeneste.
- Bedrifter som må endre sine informasjonssystemer på en slik måte at IdMegler benyttes for å koble kontekst til arbeidsprosesser, transaksjoner og informasjon.
- Offentlige registre for etablering av tjenester knyttet til tilgang til informasjon. Dette vil spesielt gjelde Folkeregisteret og Organisasjonsregisteret.
- Datatilsynet og andre myndighetsfunksjoner som politi, skatteetat, direktorater
- Personer som det er registrert informasjon om

Teknologien kan benyttes både internt i virksomheter, men kan også i sin ytterste form tilby en felles meglingstjeneste for hele samfunnet.

A.7 Organisering

IdMegler som tjeneste kan etableres som ett samarbeid mellom offentlig og private virksomheter. Det fulle potensialet av tjenesten vil fra ett personvernssynspunkt, være å etablere en kobling mellom MinSide, IdMegler (med logger) og alle virksomheter som benytter IdMegler.

IdMegler som teknologi bør utvikles og forvaltes av et eget selskap eller organisasjon som etableres som ett samarbeid mellom det offentlige, private virksomheter og representanter for befolkningen (politikere, forbruksråd?).

B Spørreundersøkelse

B.1 Spørrundersøkelse Nokios

Spørreundersøkelse personvernsarkitektur

Formålet med spørrundersøkelsen er å få mer informasjon om dagens løsninger og holdninger til personvern i ulike virksomheter, samt se på muligheter og behov for fremtidige løsninger. Gjennom arbeidet med min masteroppgave på NTNU foreslås det en tjeneste-orientert arkitektur for å etablere et skarpere skille mellom en klar autorativ kilde til personopplysninger(fysisk og logisk nivå) og for bruk av disse. En autorativ kilde til personopplysninger vil øke kvaliteten på (person)informasjon, samt muliggjøre og forbedre prosesser rundt sikkerhet og vedlikehold.

Personvern handler i første omgang om retten til å bestemme over egne personopplysninger, men også individers rett til å påvirke bruk og spredning av personopplysninger om seg selv. Dermed vil det være fordelaktig å håndtere og vedlikeholde personopplysninger i et eget register. Bruk av personopplysningene i registret vil gjøres gjennom sporbare integrasjoner med systemet. Hovedmålet med oppgaven vil derfor være å se på muligheten for å etablere en personvernsinfrastruktur, -arkitektur og -tjeneste.

Kryss av om du er interessert i å;
□ delta på et oppfølgingsintervju?
□ motta den endelige rapporten?

Mailadresse (Frivillig): _____

Tusen takk for din deltakelse! Svarene dine vil være verdifulle i utarbeidelsen av masteroppgaven min. Dersom du ønsker å motta den endelige masteroppgaven i juni 2013, send en epost til; hildevd@stud.ntnu.no

Tema:

Personlig bakgrunn

Ditt kjønn:

□Kvinne □ Mann

Din alder:

□ < - 25 år □ 25 - 35 år □ 35 - 45 år □ 45 - 55 år □ 55 - 65 år □ > 65 år +

Din høyest gjennomførte utdanning:

□ Videregående skole □ Bachelor eller tilsvarende □ Master eller tilsvarende □ Doktorgrad eller tilsvarende

Ditt arbeidssted/virksomhet:

□ Offentlig sektor □ Privat sektor □ Selvstendig næringsdrivende □ Student □ Annet, spesifiser:_____

Din rolle i virksomheten:

□ Saksbehandler □ IT-ansvarlig □ Jurist □ Administrasjon □ Annet, spesifiser:_____

Behandler din rolle personopplysninger som er regulert i henhold til Personopplysningsloven?

□ Ja □ Nei □ Annet, spesifiser:_____

Er du aktiv i sosiale medier?

□ Ja □ Nei □ Vet ikke

Hvis Ja, kryss av aktuelle sosiale mediene du benytter:

□ Facebook □ Twitter □ Linkedin □ Google + □ Myspace □ Wikipedia

Virksomhetens bakgrunn

Hvor mange ansatte er det totalt i virksomheten(Norge)?

□ < 100 □ 101 - 500 □ 501 - 1000 □ 1001 - 5000 □ > 5001

Hvor mange ansatte er det i din lokale enhet?

□ < 10 □ 11 - 50 □ 51 - 100 □ > 101

Hvilke typiske kunder har virksomheten?

□ Offentlig virksomheter □ Bedrifter □ Ideelle organisasjoner □ Personer □ Annet

Hvor mange klienter yter virksomheten tjenester til?

□ < 100 □ 101 - 500 □ 501 - 1000 □ 1001 - 5000 □ > 5001

Behandler og lagrer virksomheten personopplysninger om kunder?

□ Ja □ Nei □ Vet ikke

Hvilke type personopplysninger behandler og lagrer virksomheten i forhold til kunder?

□ Alminnelige □ Sensitive □ Annet, spesifiser:_____

Tema: Personvern

Ranger følgede spørsmål på en skala fra 1-6 hvor 6 er i veldig stor grad og 1 er i veldig liten grad. N/A er spørsmål man ikke kan besvare.

1. Virksomhetens holdninger til personvern

I hvor stor grad	1.	2.	3.	4.	5.	6.	N/A
fokuserer virksomheten på personvern?							
tar de ansatte i virksomheten hensyn til personvern?							

2. Har virksomheten retningslinjer(politikk) for personvern?

   □ Ja □ Nei □ Vet ikke

   (a) Hvis Ja,

      i. Har du satt deg inn i retningslinjene?
      □ Ja □ Nei □ Vet ikke

      ii. Tror du andre i enheten din har satt seg inn i retningslinjene?
      □ Ja □ Nei □ Vet ikke

      iii. Hvordan ble retningslinjene formidlet til ansatte i virksomheten?
      □ Obligatorisk kurs □ Frivillig kurs □ Foredrag □ Informasjonsskriv □ Mail
      □ Annet

   (b) Hvis Nei,

      i. Har virksomheten planer om utvikle retningslinjer(politikk) for personvern i nærmeste fremtid?
      □ Ja □ Nei □ Vet ikke

3. Har virksomheten retningslinjer(politikk) for informasjonssikkerhet?

   □ Ja □ Nei □ Vet ikke

   (a) Hvis Ja,

      i. Har du satt deg inn i disse?
      □ Ja □ Nei □ Vet ikke

      ii. Tror du andre i enheten din har satt seg inn i disse?
      □ Ja □ Nei □ Vet ikke

      iii. Hvordan ble disse formidlet til ansatte i virksomheten?
      □ Obligatorisk kurs □ Frivillig kurs □ Foredrag □ Informasjonsskriv □ Mail
      □ Annet

   (b) Hvis Nei,

      i. Har virksomheten planer om utvikle politikk/retningslinjer for informasjonssikkerhet?
      □ Ja □ Nei □ Vet ikke

4. Er alle ansatte i virksomheten underlagt taushetsplikt?

   □ Ja □ Nei □ Vet ikke

(a) Hvis Ja,

i. Har du signert erklæring om taushetsplikt?
□ Ja □ Nei □ Vet ikke

5. Dine holdninger til egenskaper ved personvern

I hvor stor grad	1.	2.	3.	4.	5.	6.	N/A
er personvern viktig for deg personlig?							
har du kjennskap om personvern?							
er du redd for å bli utsatt for brudd på personvernet?							
er det foretrukket at det offentlige har store personregistre?							
er det foretrukket at det private har store personregistre?							

6. Ranger viktigheten til følgende aspekter på en skala fra 1 til 3 i forhold til personvern og informasjonssikkerhet.

□ Konfidensialitet □ Integritet □ Tilgjengelighet

7. Er informasjonsikkerhet viktigere enn brukervennlighet for et system?

□ Ja □ Nei □ Vet ikke

Tema: Personopplysningsloven

Ranger følgede spørsmål på en skala fra 1-6 hvor 6 er i veldig stor grad og 1 er i veldig liten grad. N/A er spørsmål man ikke kan besvare.

8. Virksomhetens holdninger til Personopplysningsloven

I hvor stor grad	1.	2.	3.	4.	5.	6.	N/A
forholder virksomheten seg aktivt til Personopplysningsloven?							
har ansatte i virksomheten kjennskap til Personopplysningsloven?							
er Personopplysningsloven lett å etterleve?							

9. Har virksomheten direkte retningslinjer for å følge Personopplysningsloven?

□ Ja □ Nei □ Vet ikke

10. Virksomhetens kjennskap til Datatilsynet og Post- og teletilsynet

I hvor stor grad	1.	2.	3.	4.	5.	6.	N/A
har virksomheten kjennskap til Datatilsynet og Datatilsynets rolle?							
ville virksomheten forholdt seg til bransjenormer utviklet i samarbeid med Datatilsynet for å tilrettelegge for personvern?							
meldes personregister til Datatilsynet?							

11. Har det vært tilsynssaker tilknyttet Datatilsynet?

    □ Ja □ Nei □ Vet ikke

12. Har det vært tilsynssaker tilknyttet Riksrevisjonen?

    □ Ja □ Nei □ Vet ikke

13. Har det vært tilsynssaker tilknyttet Post- og Teletilsynet?

    □ Ja □ Nei □ Vet ikke

Tema: Personopplysninger

14. Har virksomheten manuelle(papir) eller digitale arkiv som inneholder personopplysninger?

    □ Ja □ Nei □ Annet, spesifiser:_____

    (a) Hvis Ja, Hvordan samles informasjonen?

        □ Webbaserte systemer □ E-post □ Scanning □ Skrevet/"Tastet inn" manuelt

        □ Annet, spesifiser:_____

    (b) Hvilken form for sikkerhet benyttes ved innsamling av informasjon?

        □ SSL-sertifikat(HTTPS) □ Kryptering □ Annet, spesifiser:_____

Ranger følgede spørsmål på en skala fra 1-6 hvor 6 er i veldig stor grad og 1 er i veldig liten grad.
N/A er spørsmål man ikke kan besvare.

15. Virksomhetens innsamling og deling av personopplysninger

I hvor stor grad	1.	2.	3.	4.	5.	6.	N/A
skiller virksomheten på sensitive og ikke-sensitive personopplysninger?							
deler virksomheten personlister (personopplysninger) med andre virksomheter?							
benytter virksomheten en felles autorativ kilde for personopplysninger?							
benyttes folkeregisteret som kvalitetskontroll for personopplysninger?							

16. Benytter virksomheten en felles autorativ kilde for personopplysninger?

    □ Ja □ Nei □ Annet, spesifiser:_____

    (a) Hvis Nei, Hvor mange kilder for personopplysninger benytter virksomheten?

        □ 1 - 3 □ 4 - 8 □ 9 - 15 □ > 15 + □ Annet, spesifiser:_____

17. Har virksomheten et klart skille mellom kunde- og ansattregistre?

    □ Ja □ Nei □ Annet, spesifiser:_____

18. Virksomhetens lagring av personopplysninger

I hvor stor grad	1.	2.	3.	4.	5.	6.	N/A
lagrer virksomheten personopplysninger direkte i fagsystemer?							
skiller virksomheten på lagring av alminnelig fortrolige og strengt-fortrolige personopplysninger?							

19. Kjenner virksomheten til lovgivingen for personlig innsyn i og tilgang til personopplysninger?

    □ Ja □ Nei □ Vet ikke

20. Virksomhetens mulighet for personlig innsyn i og tilgang til personopplysninger

I hvor stor grad	1.	2.	3.	4.	5.	6.	N/A
har virksomheten retningslinjer(politikk) for håndtering av innsynsforespørsler?							
blir virksomheten bedt om innsyn i personopplysninger fra enkeltpersoner?							
blir virksomheten bedt om innsyn i personopplysninger fra andre virksomheter?							
er det tidkrevende å kartlegge en person(hvem, hva og hvor) ved innsynsforespørsel?							

21. Er det tidkrevende å kartlegge en person ved innsynsforespørsel? (F.eks. Hvem personen er? Hvor personopplysningene ligger lagret? I hvilke systemer personopplysningene er lagret?)

    □ Ja □ Nei □ Vet ikke

22. Virksomhetens forhold til sletting av personopplysninger

I hvor stor grad	1.	2.	3.	4.	5.	6.	N/A
er det opprettet internkontroll for å kontrollere at data slettes?							
sletter virksomheten personopplysninger etter tiltenkt og forespurt formål og bruk?							
slettes personopplysninger om klienter og eksterne personer som forsvinner ut av virksomheten?							

23. Har du bedt om innsyn i personopplysninger lagret om deg?

□ Ja □ Nei □ Vet ikke

Ranger følgede spørsmål på en skala fra 1-6 hvor 6 er i veldig stor grad og 1 er i veldig liten grad. N/A er spørsmål man ikke kan besvare.

24. Bruk av og forhold til dine personopplysninger

Hvor enig eller uenig er du med påstandene under	1.	2.	3.	4.	5.	6.	N/A
Jeg forventer at personopplysninger om meg ikke skal bli benyttet til andre formål enn det jeg har gitt samtykke til.							
Jeg er redd for at andre skal få tilgang til personopplysninger lagret om meg.							
Jeg er redd for at personopplysninger om meg skal bli benyttet uten mitt samtykke.							
Jeg mener det er en fordel at personinformasjon frikobles fra personidentitet.							
Jeg har tatt snarveier som bryter med Personopplysningsloven							
Jeg mener datakriminalitet vil reduseres ved innføring av et skarpere skille mellom en klar autorativ kilde til personopplysninger og bruk.							

Tema: Bruk av personnummer

25. Benyttes personnummer som personidentitet i virksomhetens systemer?

□ Ja □ Nei □ Vet ikke

(a) Hvis ja, hvilken personidentitet benyttes for personer uten personnummer?

□ D-nummer □ Fabrikerte personnummer □ Unik nøkkel □ Annet, spesifiser:_____

(b) Hvis nei, hvilken identifisering benyttes for personidentitet?

□ Fødselsdato □ Navn □ Ansattnummer □ Annet, spesifiser:_____

Tema: Virksomhetens systemer

Ranger følgede spørsmål på en skala fra 1-6 hvor 6 er i veldig stor grad og 1 er i veldig liten grad. N/A er spørsmål man ikke kan besvare.

26. Virksomhetens autorisering i/for systemene

I hvor stor grad	1.	2.	3.	4.	5.	6.	N/A
benyttes ulike roller for å gi tilgang til og autorisering i systemene?							
har ansatte i virksomheten tilgang til systemer som inneholder personopplysninger?							
kreves det autentisering og bestemte roller for å tilgang til personopplysninger?							

27. Virksomhetens fagsystemer

I hvor stor grad	1.	2.	3.	4.	5.	6.	N/A
må personopplysninger være tilgjengelig for fagsystemene?							
spres personopplysninger mellomfagsystemer for bruk?							
lagres personopplysninger direkte i fagsystemene?							

28. Virksomhetens kontroll og oppfølging av systemene

I hvor stor grad	1.	2.	3.	4.	5.	6.	N/A
har virksomheten opprettet systemer for internkontroll/internrevisjon av Personopplysningsloven?							
har virksomheten interne regler i forbindelse ved behandling av personopplysninger?							
har virksomheten systemematisk oversikt over personopplysninger som behandles internt i systemene?							
har virksomheten internrevisjon i systemer som behandler personopplysninger?							
benytter virksomheten logging av brukernes aktivitet i forbindelse ved behandling av personopplysninger?							

Tema: Systemenes saksbehandlingsdata

Mange virksomheter behandler personopplysninger i sine systemer, men også saksbehandlingsdata, som for eksempel banktransaksjoner, kjøp eller salg for å nevne noen.

Ranger følgede spørsmål på en skala fra 1-6 hvor 6 er i veldig stor grad og 1 er i veldig liten grad. N/A er spørsmål man ikke kan besvare.

29. Henter virksomheten inn saksbehandlingsdata?

□ Ja □ Nei □ Vet ikke

30. Lagrer virksomheten saksbehandlingsdata skilt fra annen informasjon (Feks. personopplysninger)?

□ Ja □ Nei □ Vet ikke

31. Virksomhetens personopplysninger og saksbehandlingsdata

I hvor stor grad	1.	2.	3.	4.	5.	6.	N/A
behandler virksomheten saksbehandlingsdata?							
lagres personopplysninger og saksbehandlingsdata i samme database?							
behandler virksomheten personopplysninger og saksbehandlingsdata i samme system?							
behandles saksbehandlingsdata som krever personopplysninger?							
behandles saksbehandlingsdata som krever koblinger til personopplysninger?							
kobles saksbehandlingsdata med personopplysninger gjennom systemet?							
benyttes unik nøkkel for kobling mellom saksbehandlingsdata og personopplysninger?							

Tema: Offentlige mot Private virksomheter

Ranger følgede spørsmål på en skala fra 1-6 hvor 6 er i veldig stor grad og 1 er i veldig liten grad. N/A er spørsmål man ikke kan besvare.

32. Ditt forhold til offentlige i forhold til Private virksomheter

Hvor enig eller uenig er du med påstandene under	1.	2.	3.	4.	5.	6.	N/A
Jeg stoler mer på offentlige enn private virksomheter ved lagring av personopplysninger							
Jeg mener at offentlige virksomheter har mer fokus på sikkerhet rundt personinformasjon enn private virksomheter							
Jeg mener at offentlige virksomheter behandler personopplysninger med omhu							
Jeg mener at private virksomheter behandler personopplysninger med omhu							
Jeg mener det er viktig å ha større fokus på sikkerhet ved lagring av klientinformasjon enn interne personopplysninger							

Tema: Fremtidige løsninger

Regjeringen jobber med utarbeidelsen av et nytt Folkeregister. Dette sammen med innføringen av Datalagringsdirektivet vil påvirke nesten alle virksomheter i Norge, samt deres systemer og rutiner.

Ranger følgede spørsmål på en skala fra 1-6 hvor 6 er i veldig stor grad og 1 er i veldig liten grad. N/A er spørsmål man ikke kan besvare.

33. Virksomhetens fremtidige personvern

I hvor stor grad	1.	2.	3.	4.	5.	6.	N/A
vil det være viktig å illustrere nytten av innebygget personvern i nyutvikling av saksbehandlingssytemer?							
vil konsekvensvurdering for personvern være viktig?							
vil lovmessig forankring av personvernkonsekvenser være viktig?							
vil forskning på personvernsfremmende teknologi være viktig?							

34. Virksomhetens fremtidige kilde for personopplysninger

I hvor stor grad	1.	2.	3.	4.	5.	6.	N/A
kan det være fordelaktig å splitte saksbehandlingsdata og personopplysninger?							
vil det være aktuelt å abonnere på personopplysninger fra en autorativ kilde(Feks. Folkeregisteret)?							
er virksomhetenes fag- og saksbehandlingsystemer egnet for integrering mot en autorativ kilde?							
vil en autorativ kilde til personopplysninger øke effektiviteten og kvaliteten til saksbehandlingssystemene?							
har virksomheten behov for eget personregister?							
har virksomheten behov for andre registre enn folkeregisteret?							
kan det være fordelaktig å abonnere på et sentralt personregister?							
kommer virksomheten til å bli påvirket av innføringen av nytt folkeregister og personnummer?							

35. Ranger de største kostnadene ved innføring av en ny løsning (arkitektur) på en skala fra 1 til 3.

    □ Oppgradering av gamle systemer □ Anskaffelse av nye systemer □ Anskaffelse av nytt utstyr □ IT-porteføljer □ Infrastruktur □ Mange(antall) systemer som må tilpasses/endres

    □ Annet, spesifiser:_____

    (a) Hvem bør dekke disse kostnadene?

        □ Myndighetene □ Hver enkelt virksomhet □ Bør deles mellom myndighetene og hver enkelt virksomhet

        □ Annet, spesifiser:_____

36. Ranger de største risikoene ved innføring av en ny løsning (arkitektur) på en skala fra 1 til 3.

37. Ranger de mest tidkrevende faktorene ved innføring av en ny løsning (akitektur) på en skala fra 1 til 3.

38. Ranger de sørste teknologiske utfordringene ved innføring av en ny løsning (arkitektur) på en skala fra 1 til 3.

□ Komplekse systemer □ Mange avhengigheter i systemene □ Store datamengder

□ Annet, spesifiser:_____

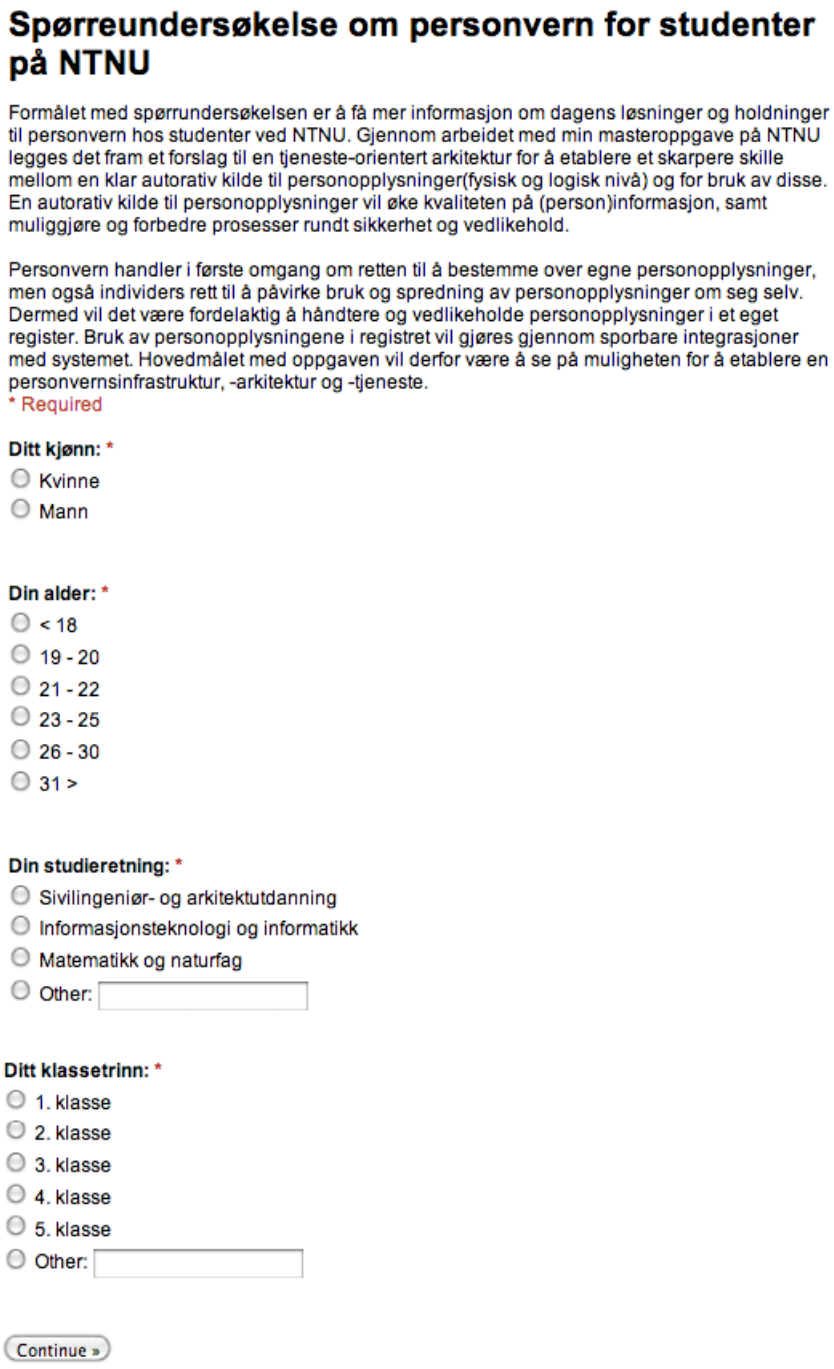
39. Virksomhetens fremtidstanker og muliggjøring av andre løsninger

I hvor stor grad	1.	2.	3.	4.	5.	6.	N/A
vil en ny løsning (arkitektur) muliggjøre lagring i Cloud, samt behandlig av større datamengder?							
vil PET(Privacy-Enhancing technologies)/personvernøkende teknologi være i fokus i fremtidsplanene?							
vil innebygd personvern som et sentralt element i virksomheten gi brukerne større tillit til systemene i fremtiden?							
vil virksomheten oppnå bedre ytelse som resultat av en ny løsning (arkitektur)?							
tror du en autorativ kilde til personopplysninger kan muliggjøre kontroll og oppføling av DLD?							

Tusen takk for din deltakelse! Svarene dine vil være verdifulle i utarbeidelsen av masteroppgaven min. Dersom du ønsker å motta den endelige masteroppgaven i juni 2013, send en epost til; hildevd@stud.ntnu.no

B.2 Spørreundersøkelse for studenter på NTNU

B.2.1 Endelig utforming av spørreundersøkelse for studenter på NTNU



Spørreundersøkelse om personvern for studenter på NTNU

Formålet med spørrundersøkelsen er å få mer informasjon om dagens løsninger og holdninger til personvern hos studenter ved NTNU. Gjennom arbeidet med min masteroppgave på NTNU legges det fram et forslag til en tjeneste-orientert arkitektur for å etablere et skarpere skille mellom en klar autorativ kilde til personopplysninger(fysisk og logisk nivå) og for bruk av disse. En autorativ kilde til personopplysninger vil øke kvaliteten på (person)informasjon, samt muliggjøre og forbedre prosesser rundt sikkerhet og vedlikehold.

Personvern handler i første omgang om retten til å bestemme over egne personopplysninger, men også individers rett til å påvirke bruk og spredning av personopplysninger om seg selv. Dermed vil det være fordelaktig å håndtere og vedlikeholde personopplysninger i et eget register. Bruk av personopplysningene i registret vil gjøres gjennom sporbare integrasjoner med systemet. Hovedmålet med oppgaven vil derfor være å se på muligheten for å etablere en personvernsinfrastruktur, -arkitektur og -tjeneste.

* Required

Ditt kjønn: *

- Kvinne
- Mann

Din alder: *

- < 18
- 19 - 20
- 21 - 22
- 23 - 25
- 26 - 30
- 31 >

Din studieretning: *

- Sivilingeniør- og arkitektutdanning
- Informasjonsteknologi og informatikk
- Matematikk og naturfag
- Other:

Ditt klassetrinn: *

- 1. klasse
- 2. klasse
- 3. klasse
- 4. klasse
- 5. klasse
- Other:

Continue »

Figur B.1: Side 1, Demografi

Spørreundersøkelse om personvern for studenter på NTNU

Side 2 av 4

Dine holdninger og kjennskap til egenskaper ved personvern

Ranger følgede spørsmål på en skala fra 1-6 hvor 6 er i veldig stor grad og 1 er i veldig liten grad. N/A er spørsmål man ikke kan besvare.

I hvor stor grad er personvern viktig for deg personlig?

	1	2	3	4	5	6	
Veldig liten grad	○	○	○	○	○	○	Veldig stor grad

I hvor stor grad har du kjennskap til personvern?

	1	2	3	4	5	6	
Veldig liten grad	○	○	○	○	○	○	Veldig stor grad

I hvor stor grad er du redd for å bli utsatt for brudd på personvernet?

	1	2	3	4	5	6	
Veldig liten grad	○	○	○	○	○	○	Veldig stor grad

I hvor stor grad har du kjennskap til Personopplysningsloven?

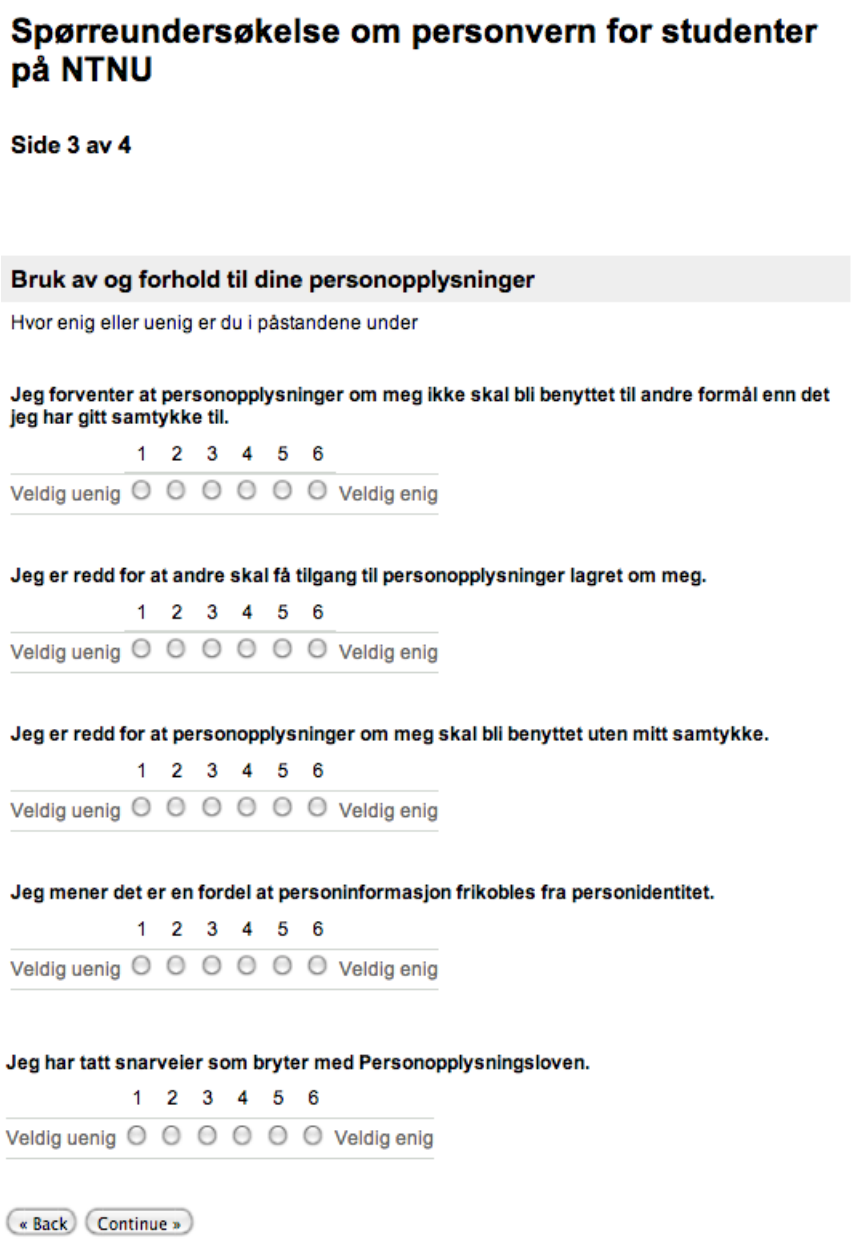
	1	2	3	4	5	6	
Veldig liten grad	○	○	○	○	○	○	Veldig stor grad

Har du bedt om innsyn i personopplysninger som er lagret om deg hos en virksomhet?

- ○ Ja
- ○ Nei
- ○ Vet ikke

« Back Continue »

Figur B.2: Side 2, Holdninger og kjennskap til egenskaper ved personvern



Spørreundersøkelse om personvern for studenter på NTNU

Side 3 av 4

Bruk av og forhold til dine personopplysninger

Hvor enig eller uenig er du i påstandene under

Jeg forventer at personopplysninger om meg ikke skal bli benyttet til andre formål enn det jeg har gitt samtykke til.

	1	2	3	4	5	6	
Veldig uenig	○	○	○	○	○	○	Veldig enig

Jeg er redd for at andre skal få tilgang til personopplysninger lagret om meg.

	1	2	3	4	5	6	
Veldig uenig	○	○	○	○	○	○	Veldig enig

Jeg er redd for at personopplysninger om meg skal bli benyttet uten mitt samtykke.

	1	2	3	4	5	6	
Veldig uenig	○	○	○	○	○	○	Veldig enig

Jeg mener det er en fordel at personinformasjon frikobles fra personidentitet.

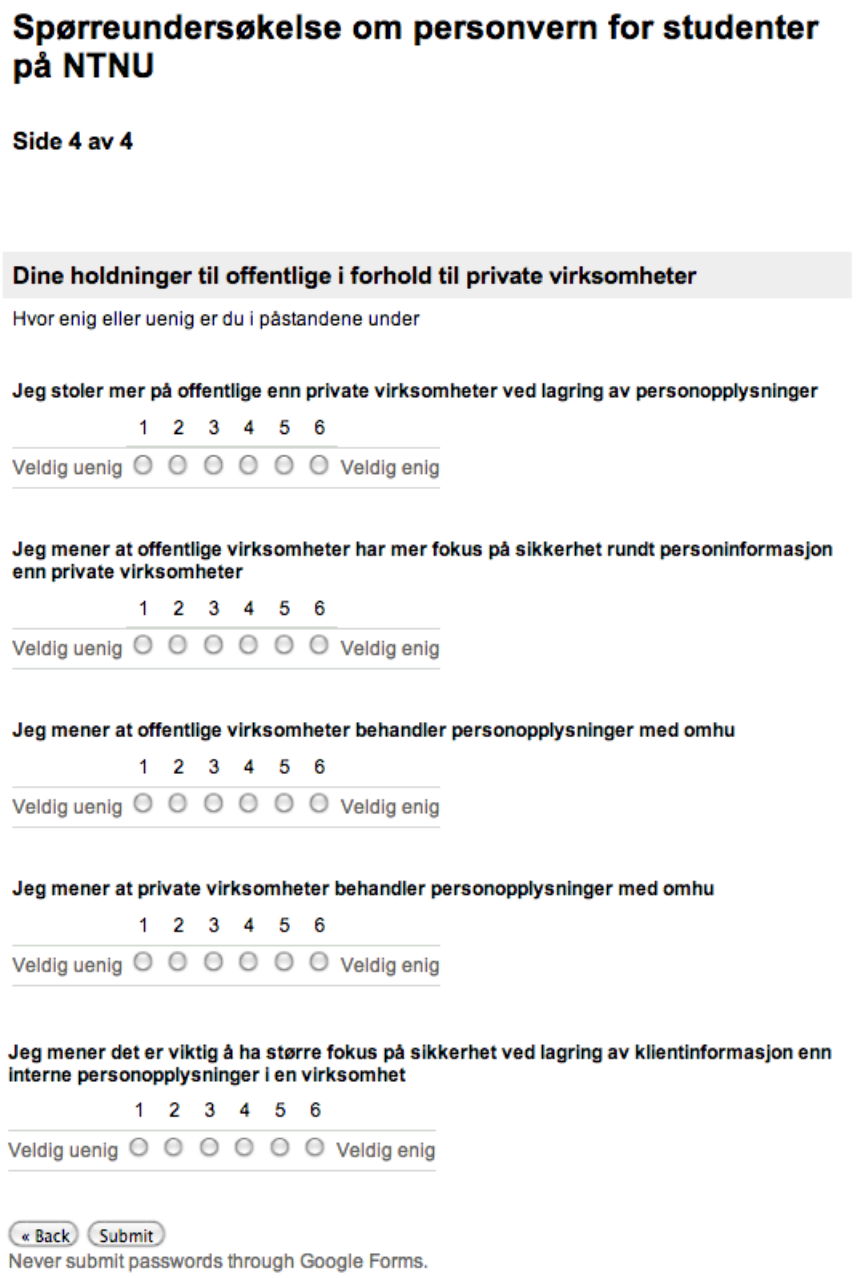
	1	2	3	4	5	6	
Veldig uenig	○	○	○	○	○	○	Veldig enig

Jeg har tatt snarveier som bryter med Personopplysningsloven.

	1	2	3	4	5	6	
Veldig uenig	○	○	○	○	○	○	Veldig enig

« Back Continue »

Figur B.3: Side 3, Bruk av og forhold til dine personopplysninger



Spørreundersøkelse om personvern for studenter på NTNU

Side 4 av 4

Dine holdninger til offentlige i forhold til private virksomheter

Hvor enig eller uenig er du i påstandene under

Jeg stoler mer på offentlige enn private virksomheter ved lagring av personopplysninger

	1	2	3	4	5	6	
Veldig uenig	○	○	○	○	○	○	Veldig enig

Jeg mener at offentlige virksomheter har mer fokus på sikkerhet rundt personinformasjon enn private virksomheter

	1	2	3	4	5	6	
Veldig uenig	○	○	○	○	○	○	Veldig enig

Jeg mener at offentlige virksomheter behandler personopplysninger med omhu

	1	2	3	4	5	6	
Veldig uenig	○	○	○	○	○	○	Veldig enig

Jeg mener at private virksomheter behandler personopplysninger med omhu

	1	2	3	4	5	6	
Veldig uenig	○	○	○	○	○	○	Veldig enig

Jeg mener det er viktig å ha større fokus på sikkerhet ved lagring av klientinformasjon enn interne personopplysninger i en virksomhet

	1	2	3	4	5	6	
Veldig uenig	○	○	○	○	○	○	Veldig enig

« Back Submit

Never submit passwords through Google Forms.

Figur B.4: Side 4, Dine holdninger til offentlige i forhold til private virksomheter

B.2.2 Analyse av spørreundersøkelse for studenter på NTNU

Faktoranalyse (Pattern matrix)

Figur B.5 viser faktoranalyse basert på Direct Oblimin for analyse av spørreundersøkelser for studenter på NTNU.

Pattern Matrix[a]

	Component				
	1	2	3	4	5
Q3.2	.909				
Q3.3	.874			.106	
Q1.3	.855				
Q1.1	.654		.244	-.109	.165
Q4.1		.927			-.112
Q4.2		.915			
Q4.3		.600			.582
Q1.2			.904		
Q1.4			.861		
Q3.5	-.136			.787	.160
Q3.4			.121	.624	-.154
Q4.5	.124	.136		.589	
Q4.4		-.114			.953

Extraction Method: Principal Component Analysis.
Rotation Method: Oblimin with Kaiser Normalization.

a. Rotation converged in 6 iterations.

Figur B.5: Faktoranalyse, "Mønster matrise"

Prinsipial komponent analyse

Figur B.6 viser prinsipial komponent analyse basert på faktoranalysen.

Påstand/Spørsmål	1	2	3	4	5
Dine holdninger og kjennskap til egenskaper ved personvern					
1.1 I hvor stor grad er personvern viktig for deg personlig?	.654		.244	.109	.165
1.2 I hvor stor grad har du kjennskap til personvern?			.904		
1.3 I hvor stor grad er du redd for å bli utsatt for brudd på personvernet?	.855				
1.4 I hvor stor grad har du kjennskap til Personopplysningsloven?			.861		
Bruk av og forhold til dine personopplysninger					
3.2 Jeg er redd for at andre skal få tilgang til personopplysninger lagret om meg.	.909				
3.3 Jeg er redd for at personopplysninger om meg skal bli benyttet uten mitt samtykke.	.874			.106	
3.4 Jeg mener det er en fordel at personinformasjon frikobles fra personidentitet.			.121	.624	.154
3.5 Jeg har tatt snarveier som bryter med Personopplysningsloven*	.136			.787	.160
Holdninger til offentlige i forhold til private virksomheter					
4.1 Jeg stoler mer på offentlige enn private virksomheter ved lagring av personopplysninger		.927			.112
4.2 Jeg mener at offentlige virksomheter har mer fokus på sikkerhet rundt personinformasjon enn private virksomheter		.915			
4.3 Jeg mener at offentlige virksomheter behandler personopplysninger med omhu		.600			.582
4.4 Jeg mener at private virksomheter behandler personopplysninger med omhu		.114			.953
4.5 Jeg mener det er viktig å ha større fokus på sikkerhet ved lagring av klientinformasjon enn interne personopplysninger i en virksomhet	.124	.136		.589	.953
Eigenvalues	3.28	2.464	2.13	1.997	1.594
% av forklart varians	25.23	18.95	16.38	15.36	12.26
Alpha	.853	.810	.748	.408	-

* = spørsmål der skalaen er reversert

Figur B.6: Prinsipial komponent analyse

Beskrivende statistikk

Figur B.7 viser beskrivende statistikk etter faktoranalyse og variabelreduksjon.

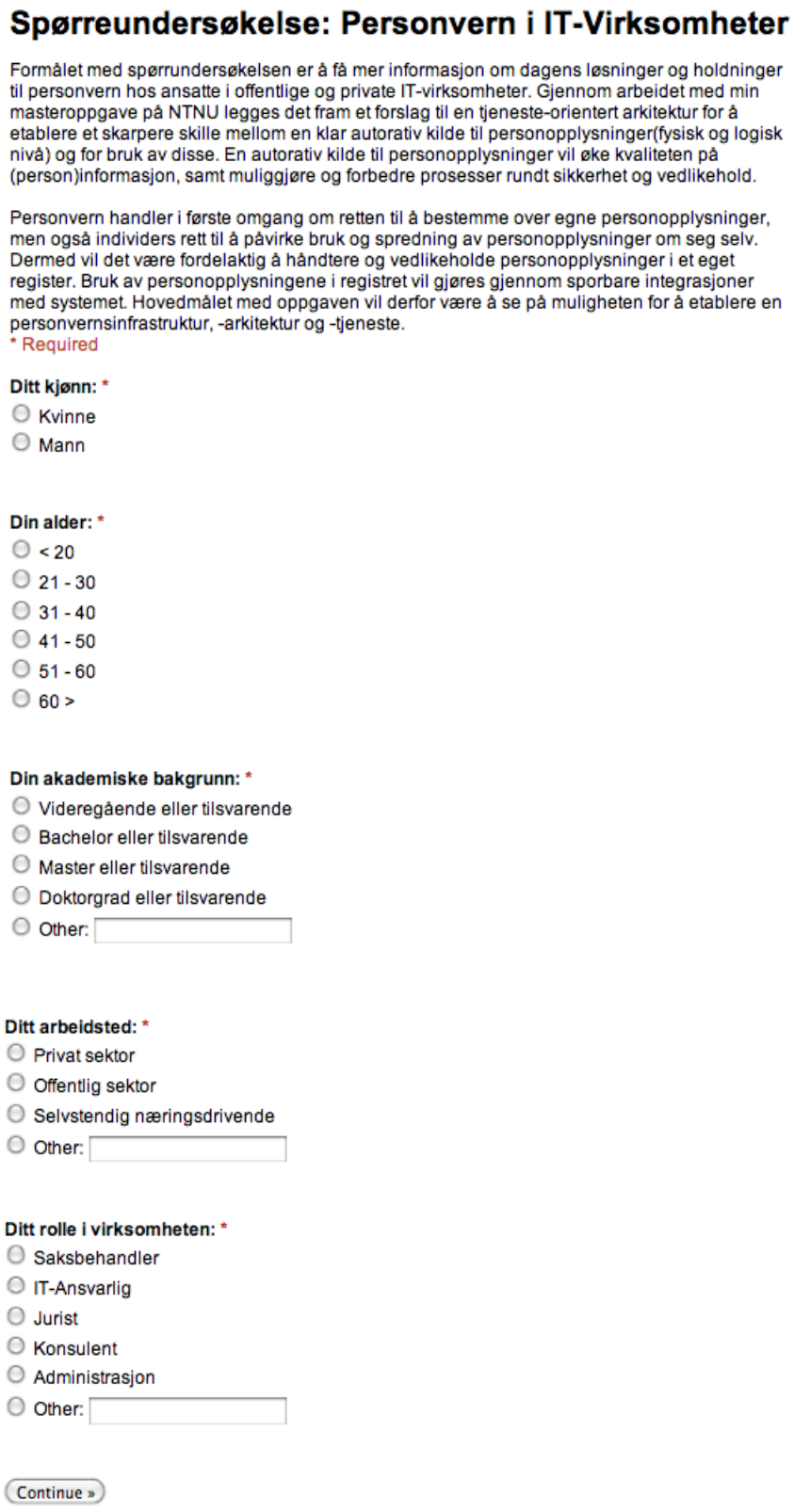
Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Kjønn	401	1	2	1.51	.501	-.025	.122	-2.009	.243
Alder	401	2	6	3.41	1.080	.548	.122	-.122	.243
Studieretning	401	1	4	2.26	1.321	.315	.122	-1.678	.243
Klassetrinn	401	1	6	2.90	1.472	.130	.122	-1.300	.243
BP	401	1.00	6.00	4.1097	1.02567	-.151	.122	-.393	.243
MP	401	1.00	7.00	3.7914	1.12791	-.167	.122	-.104	.243
KP	401	1.00	6.00	3.1696	1.09026	.479	.122	-.322	.243
Valid N (listwise)	401								

Figur B.7: Beskrivende statistikk

B.3 Spørreundersøkelse IT-virksomheter

B.3.1 Endelig utforming av spørreundersøkelse for ansatte i IT-Virksomheter



Spørreundersøkelse: Personvern i IT-Virksomheter

Formålet med spørrundersøkelsen er å få mer informasjon om dagens løsninger og holdninger til personvern hos ansatte i offentlige og private IT-virksomheter. Gjennom arbeidet med min masteroppgave på NTNU legges det fram et forslag til en tjeneste-orientert arkitektur for å etablere et skarpere skille mellom en klar autorativ kilde til personopplysninger(fysisk og logisk nivå) og for bruk av disse. En autorativ kilde til personopplysninger vil øke kvaliteten på (person)informasjon, samt muliggjøre og forbedre prosesser rundt sikkerhet og vedlikehold.

Personvern handler i første omgang om retten til å bestemme over egne personopplysninger, men også individers rett til å påvirke bruk og spredning av personopplysninger om seg selv. Dermed vil det være fordelaktig å håndtere og vedlikeholde personopplysninger i et eget register. Bruk av personopplysningene i registret vil gjøres gjennom sporbare integrasjoner med systemet. Hovedmålet med oppgaven vil derfor være å se på muligheten for å etablere en personvernsinfrastruktur, -arkitektur og -tjeneste.

* Required

Ditt kjønn: *
- Kvinne
- Mann

Din alder: *
- < 20
- 21 - 30
- 31 - 40
- 41 - 50
- 51 - 60
- 60 >

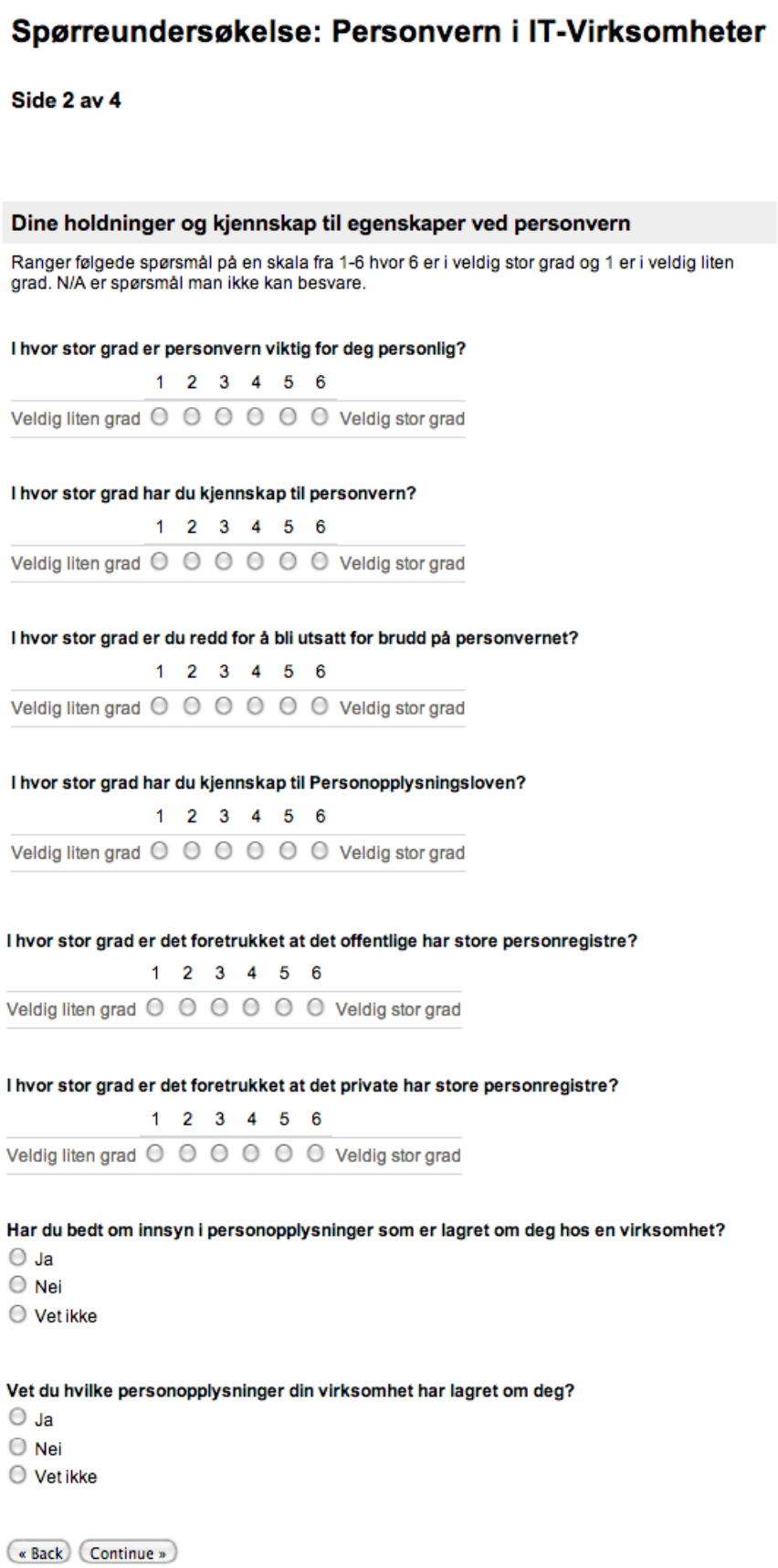
Din akademiske bakgrunn: *
- Videregående eller tilsvarende
- Bachelor eller tilsvarende
- Master eller tilsvarende
- Doktorgrad eller tilsvarende
- Other:

Ditt arbeidsted: *
- Privat sektor
- Offentlig sektor
- Selvstendig næringsdrivende
- Other:

Ditt rolle i virksomheten: *
- Saksbehandler
- IT-Ansvarlig
- Jurist
- Konsulent
- Administrasjon
- Other:

Continue »

Figur B.8: Side 1, Demografi



Spørreundersøkelse: Personvern i IT-Virksomheter

Side 2 av 4

Dine holdninger og kjennskap til egenskaper ved personvern

Ranger følgede spørsmål på en skala fra 1-6 hvor 6 er i veldig stor grad og 1 er i veldig liten grad. N/A er spørsmål man ikke kan besvare.

I hvor stor grad er personvern viktig for deg personlig?

	1	2	3	4	5	6	
Veldig liten grad	○	○	○	○	○	○	Veldig stor grad

I hvor stor grad har du kjennskap til personvern?

	1	2	3	4	5	6	
Veldig liten grad	○	○	○	○	○	○	Veldig stor grad

I hvor stor grad er du redd for å bli utsatt for brudd på personvernet?

	1	2	3	4	5	6	
Veldig liten grad	○	○	○	○	○	○	Veldig stor grad

I hvor stor grad har du kjennskap til Personopplysningsloven?

	1	2	3	4	5	6	
Veldig liten grad	○	○	○	○	○	○	Veldig stor grad

I hvor stor grad er det foretrukket at det offentlige har store personregistre?

	1	2	3	4	5	6	
Veldig liten grad	○	○	○	○	○	○	Veldig stor grad

I hvor stor grad er det foretrukket at det private har store personregistre?

	1	2	3	4	5	6	
Veldig liten grad	○	○	○	○	○	○	Veldig stor grad

Har du bedt om innsyn i personopplysninger som er lagret om deg hos en virksomhet?

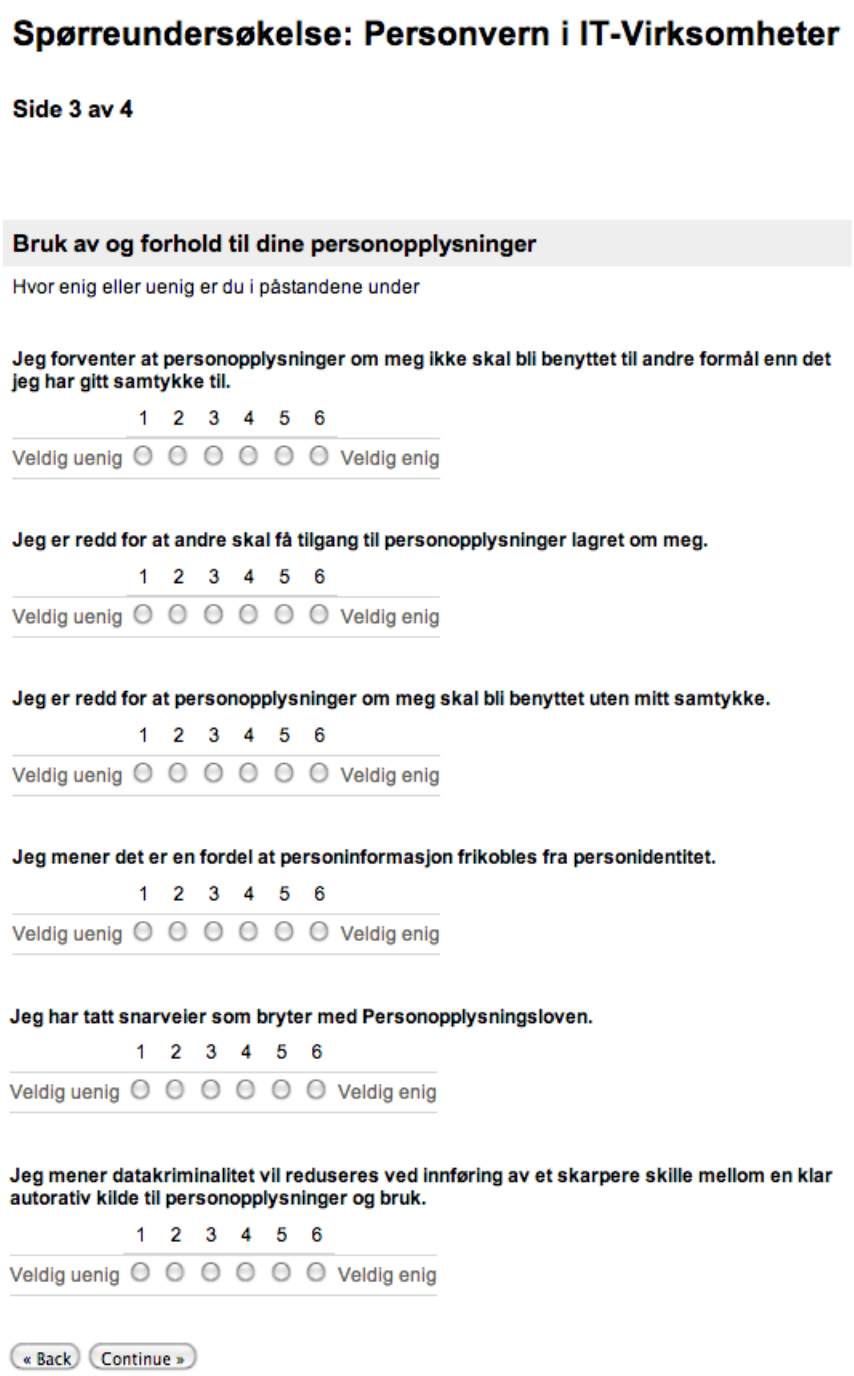
- ○ Ja
- ○ Nei
- ○ Vet ikke

Vet du hvilke personopplysninger din virksomhet har lagret om deg?

- ○ Ja
- ○ Nei
- ○ Vet ikke

« Back Continue »

Figur B.9: Side 2, Holdninger og kjennskap til egenskaper ved personvern



Spørreundersøkelse: Personvern i IT-Virksomheter

Side 3 av 4

Bruk av og forhold til dine personopplysninger

Hvor enig eller uenig er du i påstandene under

Jeg forventer at personopplysninger om meg ikke skal bli benyttet til andre formål enn det jeg har gitt samtykke til.

	1	2	3	4	5	6	
Veldig uenig	○	○	○	○	○	○	Veldig enig

Jeg er redd for at andre skal få tilgang til personopplysninger lagret om meg.

	1	2	3	4	5	6	
Veldig uenig	○	○	○	○	○	○	Veldig enig

Jeg er redd for at personopplysninger om meg skal bli benyttet uten mitt samtykke.

	1	2	3	4	5	6	
Veldig uenig	○	○	○	○	○	○	Veldig enig

Jeg mener det er en fordel at personinformasjon frikobles fra personidentitet.

	1	2	3	4	5	6	
Veldig uenig	○	○	○	○	○	○	Veldig enig

Jeg har tatt snarveier som bryter med Personopplysningsloven.

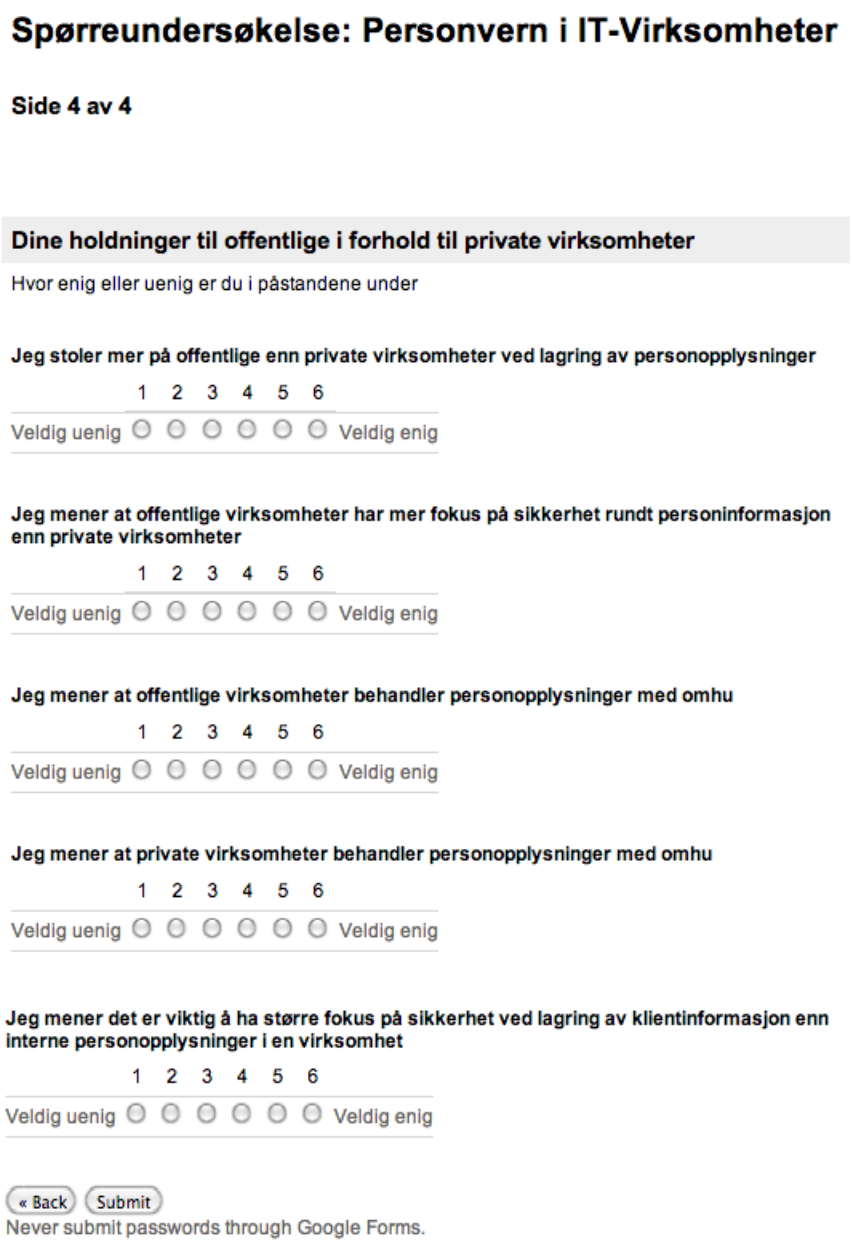
	1	2	3	4	5	6	
Veldig uenig	○	○	○	○	○	○	Veldig enig

Jeg mener datakriminalitet vil reduseres ved innføring av et skarpere skille mellom en klar autorativ kilde til personopplysninger og bruk.

	1	2	3	4	5	6	
Veldig uenig	○	○	○	○	○	○	Veldig enig

« Back Continue »

Figur B.10: Side 3, Bruk av og forhold til dine personopplysninger



Spørreundersøkelse: Personvern i IT-Virksomheter

Side 4 av 4

Dine holdninger til offentlige i forhold til private virksomheter

Hvor enig eller uenig er du i påstandene under

Jeg stoler mer på offentlige enn private virksomheter ved lagring av personopplysninger

	1	2	3	4	5	6	
Veldig uenig	○	○	○	○	○	○	Veldig enig

Jeg mener at offentlige virksomheter har mer fokus på sikkerhet rundt personinformasjon enn private virksomheter

	1	2	3	4	5	6	
Veldig uenig	○	○	○	○	○	○	Veldig enig

Jeg mener at offentlige virksomheter behandler personopplysninger med omhu

	1	2	3	4	5	6	
Veldig uenig	○	○	○	○	○	○	Veldig enig

Jeg mener at private virksomheter behandler personopplysninger med omhu

	1	2	3	4	5	6	
Veldig uenig	○	○	○	○	○	○	Veldig enig

Jeg mener det er viktig å ha større fokus på sikkerhet ved lagring av klientinformasjon enn interne personopplysninger i en virksomhet

	1	2	3	4	5	6	
Veldig uenig	○	○	○	○	○	○	Veldig enig

« Back Submit

Never submit passwords through Google Forms.

Figur B.11: Side 4, Dine holdninger til offentlige i forhold til private virksomheter

B.3.2 Analyse av spørreundersøkelse for ansatte i IT-Virksomheter

Faktoranalyse (Pattern Matrix)

Figur B.12 viser faktoranalyse baser på Direct Oblimin for analyse av spørreundersøkelse for ansatte i IT-Virksomheter.

Pattern Matrix[a]

	Component							
	1	2	3	4	5	6	7	8
Q2.3	.942							-.113
Q2.2	.896	-.208						
Q2.4	.690	.399			.192		-.236	-.215
Q1.3	.620			.274	-.259		-.122	.339
Q3.2		.962			-.123		.107	
Q3.3		.832			-.112		-.204	.162
Q3.1	-.170	.606		.324	.101	.141	.133	-.173
Q1.7			.933	-.214		-.246		
Q2.6		.194	.639		.623	.126	.198	.105
Q1.8	.404		-.509	-.427	.137	-.169		
Q1.2			-.108	.845	.159		-.179	-.148
Q1.4				.815	-.176			
Q1.1	.364		-.120	.552	.303	-.261		.146
Q2.1		-.260	-.133		.898			
Q3.5			-.172	-.167	.116	.943	-.136	
Q1.5					.174	-.252	.903	
Q1.6	.181	-.106			-.387	.459	.639	.144
Q3.4								.938
Q2.5	.164	-.195	.394	.197		.499		-.536

Extraction Method: Principal Component Analysis.
Rotation Method: Oblimin with Kaiser Normalization.

a. Rotation converged in 22 iterations.

Figur B.12: Faktoranalyse, "Mønster matrise"

C Intervjuguide

Intervjuguidene utviklet og benyttet i forbindelse med dybdeintervjuene hadde en felles introduksjon etterfulgt av virksomhetsspesifikke spørsmål, i tillegg til en felles avsluttning.

C.1 Introduksjon/Innledning

Presentasjon av meg selv:
Mitt navn er Hilde Visthoff Drange, jeg studerer til vanlig 2. master i Informatikk, med spesialisering i Systemarbeid og MMI (nå: Software) ved NTNU. Jeg er nå i gang med masteroppgaven min om Personvernsarkitektur som skal leveres våren 2013.

Informasjon om prosjektet:
Formålet med interjuvet er å få mer (tildels detaljert) informasjon om dagens tekniske arkitekturløsninger rettet mot personvern i IT-virksomheter. Gjennom arbeidet med min masteroppgave på NTNU legges det fram et forslag til en tjeneste-orientert arkitektur for å etablere et skarpere skille mellom et felles personopplysningsregister/database(en klar autorativ kilde til personopplysninger)(fysisk og logisk nivå) og for bruk av disse. Et felles personopplysningsregister/database (En autorativ kilde til personopplysninger) vil øke kvaliteten på (person)informasjon, samt muliggjøre og forbedre prosesser rundt sikkerhet og vedlikehold.

Personvern handler i første omgang om retten til å bestemme over egne personopplysninger, men også individers rett til å påvirke bruk og spredning av personopplysninger om seg selv. Dermed vil det være fordelaktig å håndtere og vedlikeholde personopplysninger i et eget register. Bruk av personopplysningene i registret vil gjøres gjennom sporbare integrasjoner med systemet.

Hovedmålet med oppgaven vil derfor være å se på muligheten for å etablere en personvernsinfrastruktur, -arkitektur og -tjeneste (ved hjelp av IdMegler).

Konsekvenser av resultatet/ Tilbakemelding resultat
Svarene fra intervjuet vil bli bearbeidet og resultatet vil bli benyttet som et utgangspunkt til å videreutvikle en mulig teknisk løsning.

Garantere anonymitet/ Spørre om mulighetene for opptak
All informasjon vil bli anonymisert og verken du eller virksomheten vil bli nevnt i oppgaven.

Retten til å bryte når som helst
Jeg vil også opplyse om at du har rett til å bryte intervjuet når som helst.

C.1.1 Faktaspørsmål (Demografi)

Starter med litt informasjon om din bakgrunn;

1. Ditt kjønn:

   □Kvinne □ Mann

2. Din alder:

   □ < - 25 år □ 25 - 35 år □ 35 - 45 år □ 45 - 55 år □ 55 - 65 år □ > 65 år +

3. Din akademiske bakgrunn:

   □ Videregående skole □ Bachelor eller tilsvarende □ Master eller tilsvarende

   □ Doktorgrad eller tilsvarende

4. Ditt arbeidssted/virksomhet:

   □ Offentlig sektor □ Privat sektor □ Selvstendig næringsdrivende □ Student

   □ Annet, spesifiser:_____

5. Din rolle i virksomheten:

   □ Saksbehandler □ IT-ansvarlig □ Jurist □ Administrasjon □ Konsulent

   □ Annet, spesifiser:_____

6. Har du bedt om innsyn i personopplysninger som er lagret om deg hos en virksomhet?

   □Ja □ Nei □ Vet ikke

7. Vet du hvilke personopplysninger din virksomhet har lagret om deg?

   □Ja □ Nei □ Vet ikke

C.1.2 Presentasjon av løsningen - IdMegler

HOVEDFORMÅL:
IdMegler skal etableres for å gjøre identitetsmegling mellom en autoritativ kilde for personinformasjon (for eksempel Folkeregister eller bedriftsintern Personregister) og transaksjonsinformasjon relatert til personen. Dette medfører at *hovedrollen* til IdMegler er å koble sammen transaksjoner/informasjon/saksbehandlingsdata med persondata.

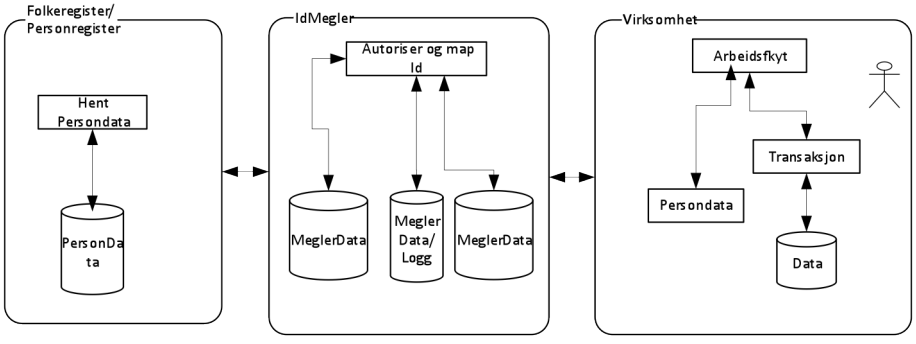
BEHOV:
Personvern handler i første omgang om retten til å bestemme over egne personopplysninger, men også individers rett til å påvirke bruk og spredning av personopplysninger om seg selv. Dermed vil det være fordelaktig å håndtere og vedlikeholde personopplysninger i ET eget register. Bruk av personopplysninger i registeret gjøres gjennom sporbare integrasjoner med systemet.

På den måte vil hver person ha;

- oversikt over hvilke informasjon som er registrert om seg selv
- mulighet til å føle eierskap til data(om seg selv) lagret hos en virksomhet
- begrense/hindre tilgang til personopplysninger lagret hos en virksomhet, basert på behov.
- tillitt til at systemer og vikrsomheter ikke misbruker lagret personinformasjon.
- mulighet til å slette data fra aktører som ikke lengre har ett (forretnings)forhold til.

FORUTSETTNINGER:

- Persondata ligger FYSISK ADSKILT fra transaksjonsdata (dvs. ikke i samme system eller database)
- Transaksjonsdata benytter generert nøkkel fra IdMegler
- IdMegler inneholder kobling til personnøkkel
- Det er ikke mulig å benytte personnøkkel for å finne transaksjoner
- Det er ikke mulig å benytte transaksjonsnøkkel for å finne personer
- Alminnelige persondata kan også frikobles personid/navn



Figur C.1: Arkitektur for IdMegler (Sørensen, 2011)

C.2 Datatilsynet

Personvernslovgiving

1. Datatilsynets rolle er å ivareta personvernslovingen til andre virksomheter på en tilfredstillende måte. Hvilke krav setter dere til egen personinformasjon?

2. Vil en løsning som IdMegler kunne ivareta personvernslovgivingen på en mer tilfredstillende måte enn dagens løsninger? Har du noen tanker om dette?

   (a) I forhold til lagring,

   (b) sletting og

   (c) innsyn i data.

DLD

3. Hvordan kan en løsning som IdMegler muliggjøre kontroll og oppfølging av DLD?

Cloud og store datasentre

Cloud: Mange utfordringer med lovgivning, men mange grunner til at man ønsker løsningen.

4. IdMegler vil muliggjøre benyttelse av cloud ved å legge mellomvaresystemet (koblingene) i skyen. Vil en ny arkitektur muliggjøre lagring og behandling av store datamengder? Hva tenker du om forholdet mellom cloud og personvern?

5. Flere og flere virksomheter velger å benytte store datasentre for lagring og prosessering av informasjon. Hva vil være datasentrenes hovedoppgave i fremtiden?

   (a) På nettsidene viser dere til en databehandleravtale i forbindelse med outsoursing ved behandling av data. Er dette tilfredstillende for å opprettholde informasjonsikkerheten og tilliten til virksomhetene og systemene? http://www.datatilsynet.no/sikkerhet-internkontroll/databehandleravtale/

C.3 Skatteetaten

Personinformasjon

1. Jeg antar at Skattetaten har store mengder personinformasjon og persondata lagret. Hvordan definerer du begrepet personinformasjon?
2. Hvordan håndterer Skatteaten personinformasjon?
3. Benyttes et felles autorativ register/database for personopplysninger?
   (a) Hvis Nei, Hvorfor ikke? Hvor mange kilder til personopplysninger benyttes?
   (b) I hvilken grad vil det være mulig å innføre en autorativ kilde til personinformasjon?
      i. Internt?
      ii. Eksternt? Et felles personopplysningsregister
4. Hva ser du på som de største fordelene/ulempene ved å benytte en autorativ kilde til personopplysninger?

Lagring av personopplysninger

5. Lagrer Skatteetaten personopplysninger direkte i fagsystemer? Må personopplysninger være tilgjengelig for fagsystemene? Hvorfor?
   (a) Hvis Ja, er personopplysningene duplikater av allerede lagret informasjon?
6. Skiller Skatteetaten på lagring av alminnelig fortrolige og strengt fortrolige personopplysninger?

Personlig innsyn i og tilgang til personopplysninger

7. Har Skatteetaten retningslinjer for håndtering av innsynsforespørsler?
8. Er det tidkrevende å kartlegge en person ved innsynsforespørsel ? (F.eks. Hvem personen er? Hvor personopplysninger ligger lagret? I hvilke systemer personopplysninger er lagret?)
9. Autentisering: I hvilken grad benyttes roller for å begrense tilgang til personinformasjon/data? Hva er fordelaktig med en slik løsning?

Sletting av personopplysninger

10. Har Skatteetaten internkontroll for å kontrollere at data slettes?

Personregistre/ Folkeregisteret

11. Skatteetaten oppbevarer et register som omfatter alle personer som bor, eller har bodd i Norge. Hvordan lagres denne informasjonen?
12. Kvalitetsikres informasjon lagret i folkeregisteret? Hvordan og evt. hvor ofte?

Store datamenger og cloud

Cloud: Mange utfordringer med lovgivning, men mange grunner til at man ønsker løsningen.

13. IdMegler vil muliggjøre benyttelse av cloud ved å legge mellomvaresystemet (koblingene) i skyen. Vil en ny arkitektur muliggjøre lagring og behandling av store datamengder? Hva tenker du om forholdet mellom cloud og personvern?

14. Flere og flere virksomheter velger å benytte store datasentre for lagring og prosessering av informasjon. Hva vil være datasentrenes hovedoppgave i fremtiden? Tror du dette er noe dere kommer til å ønske å benytte iløpet av fremtiden?

IdMegler

15. Hovedmålet med IdMegler er å frikoble personinformasjon fra saksbehandlingsdata. (Disse kobles med en tidsbestemt nøkkel generert av IdMegler.) Vil dette øke personvernet til den enkelte i hver enkelt saksbehandling?

Fremtid

16. Ved utviklingen av nye systemer, tror du det i fremtiden er behov for/ nødvendig med personregistre?

17. I forhold til folkeregisteret, tror du dette kan tas i bruk som et felle register? Ved å gjøre det mer tilgjengelig for bruk. Kan dette øke kvaliteten, unngå duplikater, kopieringer og siloer?

C.4 Difi

Personinformasjon

1. Hvordan håndterer og i hvor stor grad håndterer DIFI personinformasjon?
2. Benyttes et felles autorativ register/database for personopplysninger?
   (a) Hvis Nei, Hvorfor ikke? Hvor mange kilder til personopplysninger benyttes?
   (b) I hvilken grad vil det være mulig å innføre en autorativ kilde til personinformasjon?
      i. Internt?
      ii. Eksternt? Et felles personopplysningsregister
3. Hva ser du på som de største fordelene/ulempene ved å benytte en autorativ kilde til personopplysninger?

Lagring av personopplysninger

4. Lagrer DIFI personopplysninger direkte i fagsystemer? Må personopplysninger være tilgjengelig for fagsystemene? Hvorfor?
   (a) Hvis Ja, er personopplysningene duplikater av allerede lagret informasjon?

Personlig innsyn i og tilgang til personopplysninger

5. Er det tidkrevende å kartlegge en person ved innsynsforespørsel ? (F.eks. Hvem personen er? Hvor personopplysninger ligger lagret? I hvilke systemer personopplysninger er lagret?)
6. Autentisering: I hvilken grad benyttes roller for å begrense tilgang til personinformasjon/data? Hva er fordelaktig med en slik løsning?

Arkitekturstandarder

7. DIFI har iløpet av de siste årene utvikletet standarder for personvern og arkitektur. Hva vektlegges ved utviklingen av disse? Benytter dere disse ved utvikling av egne systemer? Internt: For dem med tilgang til lagret informasjon.
8. Hvilke prinsipper er viktigst dersom man skal utvikle en ny arkitektur som støtter personvernet?
   (a) Tjenesteorientering?
   (b) Interopabilitet?
   (c) Tilgjengelighet?
   (d) Sikkerhet?
   (e) Åpenhet?
   (f) Fleksibilitet?
   (g) Skalerbarhet?
9. Sett fra et arkitekturperspektiv: Hva er forholdet mellom personvern og informasjonssikkerhet?

Store datamenger og cloud

Cloud: Mange utfordringer med lovgivning, men mange grunner til at man ønsker løsningen.

10. IdMegler vil muliggjøre benyttelse av cloud ved å legge mellomvaresystemet (koblingene) i skyen. Vil en ny arkitektur muliggjøre lagring og behandling av store datamengder? Hva tenker du om forholdet mellom cloud og personvern?

11. Flere og flere virksomheter velger å benytte store datasentre for lagring og prosessering av informasjon. Hva vil være datasentrenes hovedoppgave i fremtiden? Tror du dette er noe dere kommer til å ønske å benytte iløpet av fremtiden?

IdMegler

11. Hovedmålet med IdMegler er å frikoble personinformasjon fra saksbehandlingsdata. (Disse kobles med en tidsbestemt nøkkel generert av IdMegler.) Tror du dette øke personvernet til den enkelte i hver enkelt saksbehandling?

Fremtid

12. Ved utviklingen av nye systemer, tror du det i fremtiden er behov for/ nødvendig med personregistre?

13. I forhold til folkeregisteret, tror du dette kan tas i bruk som et felle register? Ved å gjøre det mer tilgjengelig for bruk. Kan dette øke kvaliteten, unngå duplikater, kopieringer og siloer?

C.5 Sparebank 1 - Gruppen

Personinformasjon

1. Jeg antar at SB1-gruppen har store mengder personinformasjon og persondata lagret. Hvordan definerer dere begrepet personinformasjon?
2. Hvordan håndterer SB1-Gruppen personinformasjon?
3. Benyttes et felles autorativ register/database for personopplysninger?
   (a) Hvis Nei, Hvorfor ikke? Hvor mange kilder til personopplysninger benyttes?
   (b) I hvilken grad vil det være mulig å innføre en autorativ kilde til personinformasjon?
      i. Internt?
      ii. Eksternt? Et felles personopplysningsregister
4. Hva ser du på som de største fordelene/ulempene ved å benytte en autorativ kilde til personopplysninger?

Lagring av personopplysninger

5. Lagrer SB1-Gruppen personopplysninger direkte i fagsystemer?(Feks. i forbindelse med saksbehandling) Må personopplysninger være tilgjengelig for fagsystemene? Hvorfor?
   (a) Hvis Ja, er personopplysningene duplikater av allerede lagret informasjon?
6. Skiller SB1-Gruppen på lagring av alminnelig fortrolige og strengt fortrolige personopplysninger?

Personlig innsyn i og tilgang til personopplysninger

7. Har SB1-Gruppen retningslinjer for håndtering av innsynsforespørsler?
8. Er det tidkrevende å kartlegge en person ved innsynsforespørsel ? (F.eks. Hvem personen er? Hvor personopplysninger ligger lagret? I hvilke systemer personopplysninger er lagret?)
9. Autentisering: I hvilken grad benyttes roller for å begrense tilgang til personinformasjon/data? Hva er fordelaktig med en slik løsning?

Sletting av personopplysninger

10. Har SB1-Gruppen internkontroll for å kontrollere at data slettes? Slettes personopplysninger etter endt kundeforhold?

Cloud og store datasentre

Cloud: Mange utfordringer med lovgivning, men mange grunner til at man ønsker løsningen.

11. IdMegler vil muliggjøre benyttelse av cloud ved å legge mellomvaresystemet (koblingene) i skyen. Vil en ny arkitektur muliggjøre lagring og behandling av store datamengder? Hva tenker du om forholdet mellom cloud og personvern? Hvordan forholdere SB1-Gruppen seg til en mulig benyttelse av skytjenster? (Feks. Every har valgt å outsource drift til øst-europeiske land)

12. Flere og flere virksomheter velger å benytte store datasentre for lagring og prosessering av informasjon. Hva vil være datasentrenes hovedoppgave i fremtiden?

Store Personregistre

13. Vil det i fremtiden være mulig å benytte systemer uten egne, lokale personregistre?

C.6 Avsluttning

C.6.1 Spørsmål rettet direkte mot Forskningsspørsmålene

1. Hvordan tror du tjeneste-orientert arkitektur kan forbedre anonymiseringen av personinformasjon i forhold til Personopplysningsloven? og igjen være bidragsyter til å bekjempe identitetstyveri? Hva vil være de viktigste faktorene?

2. Personopplysningsloven setter retningslinjer for å hente ut/få innsyn i/slette informasjon om informasjon lagret om deg selv, men hvordan løses dette i praksis med dagens teknologiske løsninger? Hvilke teknologisk søtte/prosess har man som bruker av systemene?

3. Tror du det er det mulig å opprette en klar autorativ kilde til personopplysninger? Kan du utdype det nærmere?

4. Hvem eier i praksis informasjonen som er lagret hos en virksomhet om en person?

C.6.2 Generelle spørsmål

18. Kvalitetsikrer og vedlikeholder dere lagret data? Hvordan gjennomføres dette? Sjekkes opplysningene opp mot en bestemt kilde?

19. IdMegler kan også benyttes som et informasjonssystem. I den forbindelse benyttes IdMegler som et grensesnitt for kvalitetsikring og eventuell begrensning/styring av hvem som skal ha tilgang til informasjon om personen. Hva vil være de største utfordringene med en slik løsning?

Regjeringen jobber med utarbeidelsen av et nytt Folkeregister. Dette sammen med innføringen av Datalagringsdirektivet vil påvirke nesten alle virksomheter i Norge, samt deres systemer og rutiner.

20. I hvor stor grad vil det være viktig å illustrere nytten av innebygget personvern i nyutvikling av saksbehandlingssytemer?

21. I hvilke sammenhenger vil konsekvensvurdering for personvern være viktig?

22. Vil lovmessig forankring av personvernkonsekvenser være mer opplysende og konkretisere personvernslovgivingen for “Ola Normann”?

C.6.3 Avsluttende spørsmål - Andre påvirkende faktorer

Da skal jeg bare avslutte med et par korte spørsmål;

23. Hva tror du er de største kostnadene ved innføring av en ny løsning?

    - Oppgradering av gamle systemer?
    - Anskaffelse av nye systemer?
    - Anskaffelse av nytt utstyr?
    - IT-Porteføljer?
    - Infrastruktur?
    - Mange (antall) systemer som må tilpasses/endres?

    (a) Hvem bør dekke disse kostnadene?

    - Myndighetene?
    - Hver enkelt virksomhet?
    - Bør deles mellom myndighetene og hver enkelt bedrift?

24. Hva er de største risikoene ved innføring av en ny løsning(arkitektur)?

    - Drift under utvikling
    - Migrering
    - Datakvalitet

25. Hva er de mest tidkrevende faktorene ved innføring av en ny løsning (arkitektur)?

    - Ansaffelsesprosesser
    - Migrering
    - Tilpasse nye og gamle systemer

26. Hva er de største teknologiske utfordringene ved innføring av en ny løsning (arkitektur)?

    - Komplekse systemer?
    - Mange avhengigheter i systemene?
    - Store datamengder?

27. Er det noe viktig jeg ikke har spurt om? Kan jeg ta kontakt senere?

C.6.4 Avsluttning

Jeg takker deg for velvillig samarbeide og at du hadde mulighet til å delta på intervjuet. Det vil være til veldig stor hjelp for utarbeidelsen av masteroppgaven min. Jeg vil reinskrive intervjuet på grunnlag av notater og opptak. Du får tilsendt intervjuutskriften på mail i løpet av kort tid, for gjennomlesning og redigering. Setter stor pris på om du har mulighet til å gi tilbakemelding om evt feil og mangler/misforståelser. Som jeg også sa, resultatene vil være anonyme og jeg vil sende deg en kopi av masteroppgaven som takk for at du har tatt av din tid til å hjelpe meg.