Semicolon

Sjekkliste for avsender og mottaker av data.

Til bruk ved etablering og endring av elektronisk samhandling

Versjon: 1.0

Dato: 18. Desember 2012

Forfattere:

- Thom-Kåre Granli, Institutt for Privat rett, Juridisk fakultet, Universitetet i Oslo
- Terje Grimstad (Karde)
- Per Myrseth (DNVKEMA)
- Erlend Øverby (Karde)

Versjonshistorikk for dette dokumentet

Versjon & Dato	Kommentar og ansvarlig
Versjon 0,9 2. november 2012	Basert på arbeid av Thom-Kåre Granli, Terje Grimstad, Per Myrseth og Erlend Øverby.
V0.9b, 5. November 2012	Kommentar av Terje Grimstad
V 0,99, 19. November 2012	Oppdateringer basert på tilbakemeldinger. Blant lagt inn: sjekkliste for intensjonsavtalen, risikoanalysekapittelet, utvidet datakvalitet mm. Per Myrseth
V 0,99c. 27. november. 2012	Input på gevinstrealisering fra Leif Skivenes Flak. Input på språkbruk og faglige kommentarer på risikostyring fra DNVKEMA. Redigert inn av Per Myrseth.
V 0.99d 17. desember 2012	Oppdateringer basert på tilbakemeldinger i workshop hos UDI. Tilstede: Mariann Sundvor, Irene Foss, Laila Fimreite, Erlend Øverby, Thom-Kåre Granli og Per Myrseth. Redigert inn av Per Myrseth
V 1.0, 18. Desember 2012	Basert på oppdateringer etter seminar hos UDI. 17. desember 2012. Per Myrseth

Innholdsfortegnelse

1 Introduksjon

Hensikt med dette dokumentet er å gi mottaker og avsender en sjekkliste for hva de bør tenke på og eventuelt utrede når de starter samarbeid om å etablere elektronisk samhandling.

Sjekklistene for avsender og mottaker som er beskrevet i dette dokumentet må sees i sammenheng med dokumentene:

- Veiledning i bruk av maler og sjekklister [12]
- Intensjonsavtale [14]
- Utvekslingsavtale [15]
- Veiledning for bruk av avtalene [13]

Sjekklistene er ment å dekke sentrale spørsmål fra idestadiet frem til signert utvekslingsavtale. Utvekslingsavtalen med bilag beskriver bl.a. hvilken informasjon som skal utveksles for å oppnå hvilke mål. Etter signering av utvekslingsavtalen anbefaler vi at en starter design av nye arbeidsprosesser og ny IT-støtte for å realisere samhandlingen.

Viktige showstoppere for elektronisk samhandling er:

- Organisatorisk og enkeltpersoners vilje og evne til å samhandle
- Juridiske aspekter
- Budsjetter og ressurser, fraværende eller i utakt mellom etater.
- Ukjent eller lav datakvalitet
- Ukjent eller for høy risiko
- Uklart gevinstpotensial
- For lite innsalg av hvorfor elektronisk samhandling bør etableres.
- For liten vilje til å endre at borger/næringsdrivende for ofte er «brevdue» mellom offentlige etater.
- Fordeling av kostnader og uttak av gevinster mellom partene skaper ulik motivasjon for deltakelse.
- IKT, gjerne knyttet til eldre IT systemer eller tilgang på et tidsvindu for å kunne gjennomføre endringer hos flere partert koordinert.

Ansvaret for tilstrekkelig kvalitet på data som benyttes i saksbehandling ligger hos mottaker, men avsender må beskrive og avgi data slik at mottaker har mulighet til å forstå dem. Avsender har et ansvar for at avgitte data brukes i henhold til hjemler hos avsender.

Gjeldende arkitekturprinsipper for offentlig sektor er tjenesteorientering, interoperabilitet, tilgjengelighet, sikkerhet, åpenhet, fleksibilitet og skalerbarhet [19]. Semicolons sjekklister og avtaler vil hjelpe etater med å følge disse prinsippene.

En ferdig utfylt sjekkliste for både avsender og mottaker er anbefalte bilag til utvekslingsavtalen.

I tillegg til sjekklistene under, er det laget egne kapitler i dette dokumentet som beskriver viktige momenter, reiser spørsmål og gir litteraturhenvisninger som kan være relevant for etablering av elektronisk samhandling.

Veiledning til kolonnene:

- **Nr**: Er kun for identifikasjon og henvisning til spørsmålet.
- **Spørsmål**. Er basert på Semicolons arbeid med avtalene og sjekklistene. Motivasjon og forklaring til flere av spørsmålene er beskrevet i egne kapitler i dette dokumentet.
- **Ja/nei**. Avgrensning til ja eller nei som svaralternativer på spørsmålet er bevisst. Dette fordi ett nei bør fører til stopp eller utsettelse av prosjektet.
- **Dokument.** Her oppgis hvor spørsmålet er besvart, gjerne med henvisning til avtale-bilag, notat, rapport, forskrift etc.
- **Signatur & rolle**. Viser hvem som har ansvaret for at spørsmålet er tilstrekkelig utredet og at vedkommende har fullmakt og kompetanse til å besvare spørsmålet

Kolonner som kun finnes i sjekklisten for utvekslingsavtalen:

- **Kategori**. Viser hvilke av følgende kategorier det enkelte spørsmålet er knyttet til:
    - Informasjon: Fokuserer på informasjon med sin selvstendige verdi uavhengig av hvilket/hvilke IT-system som benyttes for å håndtere informasjonen. Beskrivelse av betydning og begrepsmodeller er koblet til dette laget.
    - Prosess: En etats interne prosess
    - Prosjekt: Prosjektet eller forlengelsen av prosjektet (systemutviklingsfasen evt driftsfasen) har ansvar spørsmålet.
    - Jus: Knyttet til betydning av informasjon, hjemler for å innhente, benytte, avgi, samt krav til forvaltning og sikkerhet.
    - Risikostyring: gevinstanalysen, endringsstyring, kvalitetsledelse, risikoledelse mm.
- **Mottakersjekkliste.** For hvert spørsmål i sjekklista er det kommentert om spørsmålet skal snus til å sette mottaker i sentrum eller om spørsmålsteksten kan kopiers som den står.

2 Sjekklister til intensjonsavtalen

Følgende sjekkliste bør benyttes før en inngår intensjonsavtalen.

2.1 Intensjonsavtale: Sjekkliste for Mottaker

Nr	Spørsmål	Ja/nei	Dokument	Signatur & rolle
1	Har vi budsjett for gjennomføring av planleggingsfasen?			
2	Har vi beskrevet prosessen hvor data skal anvendes?			
3	Har vi beskrevet hvilke data vi trenger?			
4	Har vi hjemmel til å spørre om data fra avsender?			
5	Har vi lov til å benytte data?			

2.2 Intensjonsavtale: Sjekkliste for Avsender

Nr	Spørsmål	Ja/nei/	Dokument	Signatur & rolle
1	Har vi aktuelle data?			
2	Er data underlagt utleverings restriksjoner?			
3	Er det hjemmel/lov til å avgi data til aktuelt formål?			
4	Kan data bli åpne data?			
5	Er det alternative kilder til sammenlignbare data?			
6	Har vi beskrevet prosessen for hvordan data blir opprettet og forvaltet?			
7	Har vi budsjett for gjennomføring av planleggingsfasen?			

3 Sjekkliste til utvekslingsavtalen

3.1 Utvekslingsavtalen, sjekklister for Avsender

Denne sjekklisten for utvekslingsavtalen forutsetter at Avsendersjekklisten for intensjonsavtale er besvart.

Nr	Kategori	Spørsmål	Ja/Nei	Dokument	Signatur & rolle	Mottaker -sjekkliste
1	Infor-masjon	Er det alternative kilder til sammenlignbare data? Om flere kilder: • Basert på hvilke kriterier ble kilde valgt? • Er samme kilde best egnet gjennom hele året/livsløpet? • Er det de faktiske verdier fra datakilden som er interessant eller kan enkle ja/nei svar eller svar på over / under terskelverdier benyttes.		Bilag 1		Kopi
2	Infor-masjon	Er de valgte opplysningstypene for utveksling beskrevet slik at mottaker enkelt kan forstå dem og anvende dem og evner IT-systemene å hente ut de aktuelle data? - Er informasjonsmodell, begrepsmodell med identifikatorer og utvekslingsmodell etablert for utvekslingen? Se kap 4.1 Beskrivelse av data. - Er det beskrevet hvor i vårt system informasjon finnes og har systemet evne til å avgi de aktuelle data på en egnet måte for mottaker?		Bilag 1 ,3		Snu sp.
3	Infor-masjon	Er følgende beskrevet på en hensiktsmessig måte for mottaker • Opphav til data? Se kap 4.2 Etablering og forvaltning, 4.3 aktiviteter & infobruk + [9] • Opphav til opplysningstyper? Er det gjort søk i SERES og evt. andre kilder om noen har beskrevet relevant felles modell/deler av modell? • Hva/hvem en har data om (populasjon)? Se 4.1.1 Populasjon. • Hvilke data (attributter) en har? Se 4.1 Beskrivelse av data. • Tilhørende forvaltningsregime? Se kap 4,7 Datakvalitet		Bilag 1, 3		Snu sp.

		• Sikkerhetskrav? Se kap 4.10 Sikkerhet				
4	Jus	Er juridiske krav og forutsetninger som avsender må forholde seg til i sin databehandling og utlevering kartlagt?		Bilag 1, 2		Snu sp.
5	Jus	Er kobling mellom aktivitetsmodell & dataflyt til jus beskrevet. Det vil si er det rettslige grunnlaget for informasjonsbehovet beskrevet?		Bilag 1, 2		Kopi
6	Prosess	Håndtering ved endring i data (klagebehandling mm). Utfordringer er å vite hvilken tilstand en opplysning er i. • Er håndtering av endringer i data beskrevet som aktiviteter mellom avsender og mottaker? • Er disse tilstander (ulike typer endringer) på data del av informasjonsmodell, begrepsmodell og utvekslingsmodell hos avsender? Håndtering ved feil i data. • Er håndtering av feilsituasjoner på data beskrevet som aktiviteter mellom avsender og mottaker? • Er disse tilstander (feil og ulike typer endringer) på data del av informasjonsmodell, begrepsmodell og utvekslingsmodell hos avsender?		Bilag 1 Bilag 4 (SLA), 5		Snu sp.
7	Prosess	Hvordan sikres tilstrekkelig datakvalitet og hva kjennetegner gjeldende minimumsnivå for datakvalitet? Se kap 4.5 Transformasjoner, 4.7 Datakvalitet og 4.9 Endringer.		Bilag 1		Kopi
8	Prosess	Er avsender og mottakers krav til datakvalitetsnivå beskrevet og harmonisert. Se 4.7 Datakvalitet og ISO 8000 [10].		Bilag 1, 4		Kopi
9	Prosess	Kan avsender forsikre seg om at mottaker forstår data korrekt? Er følgende beskrevet tilstrekkelig. • Avsenders tolkning av data? Se 4.1 Beskrivelse av data. • Mottakers tolkning av data? Se 4.1 Beskrivelse av data. • Transformering av dataformat, datastruktur og semantikk. Se 4.5 transformasjoner. Kan avsender forsikre seg om at mottaker får de opplysningene de rettslig sett har bruk for?		Bilag 1 Bilag 1, 2		Snu sp.

		Er følgende beskrevet tilstrekkelig. • Mottakers saksbehandling/ oppgaveløsning				
10	Prosess	Hvilke nye rutiner må etableres knyttet til utveksling av data? Eksempel på rutiner: • Sletterutiner internt og hos mottaker • Håndtering av logger for datautveksling • Ettersending ved feil i data • Endringer som må håndteres knyttet til omgjøringsplikt hos mottaker • Varsling ved endringer i: forskrifter, tolkning av data/begrepsmodell, programvare og bruk av data, etc. • Er ansvar for risikostyring tydelig hos de involverte Rutiner for håndtering ved feil på teknologi • Er håndtering av feilsituasjoner på teknologi beskrevet som aktiviteter mellom avsender og mottaker? • Er det tilrettelagt for test og driftsmessig overvåking av tekniske tjenester.		Bilag 1 Bilag 4 Bilag 5 Bilag 6 Bilag 4 (SLA)		Snu sp.
11	Risiko-styring	Er metodisk tilnærming og tidsplan for risikoanalyser avklart? Gjelder blant annet risikoanalyse av : • Design og etablering av datautvekslingen med tilhørende tiltak godkjent av relevant ansvarlig/ rolle? • Etablering av testmetode, testmiljø og testdata i et inter-etat testmiljø. • Er ansvar for etatsprosesser klart beskrevet og avklart. • Er ansvar for prosjektleveranser klart beskrevet og avklart. • Er ansvar for samhandlingen beskrevet og avklart. • Endringer i samhandling på ulike nivå (teknisk, organisatorisk mm.) • Forhold hos involverte parter, inkl tredjeparter • Helheten av samhandlingen • Er ansvar for risikostyring tydelig hos de involverte		Bilag 11: Mandat og prosjektplan Bilag 6		Kopi

		Se kap 4.6 Risikoanalyser og risikostyring.				
12	Risiko-styring	Er metodisk tilnærming og tidsplan for kvalitetsstyring avklart? Er rutiner for kvalitetssikring etablert hos begge parter, eksempelvis ISO 9000 el. Eksempelvis: kvalitetssikring av: • Nye rutiner for saksbehandling, informasjonsforvaltning etc. • Ny teknologi og programvare, inkl. konfigurasjonsstyring av programvare • Nye grensesnitt internt og eksternt • Systemutviklingsrutiner, testing av programvare mm • Er ansvar for risikostyring tydelig hos de involverte • Etablering av sikkerhetsmekanismer Dette må sees opp mot avtalebilagene for bl.a. prosessbeskrivelse, begrepsmodeller og hjemmel/juridiske krav.		Bilag 11: Bilag 6		Kopi
13	Risiko-styring	Er metodisk tilnærming og tidsplan for gevinstrealisering avklart? Hvordan er det planlagt å måle at gevinstanalysen som er basis for etablering av elektronisk samhandling er oppnådd og hvem er ansvarlig?		Bilag 11		Kopi
14	Prosjekt	Er innsalg og forankring av prosjektet samt etablering av budsjetter og fullmakter etablert? Gjelder for hver prosjektfase for etablering av elektronisk samhandling.		Bilag 11		Kopi
15	Prosjekt	Er planlagte tidsvindu for endringer realistisk? Er endringer i saksbehandlingsrutiner og programvare mulig å gjennomføre på ønsket tid hos (i) avsender og (ii) mottaker, (iii) tredjeparter/ASP/Cloud tjenester og/eller offentlige felleskomponenter som Altinn, SERES mm.		Bilag 11		Kopi
16	Prosjekt	Over tid endres måten vi jobber på, hvilke systemer som samvirker, hvor en mottar data fra etc. • Hvordan skal slike endringer og bieffekter som påvirker samhandlingen håndteres? • Hvem har ansvar for å fange dem opp samt ta ansvar for at de blir håndtert? • Hvordan håndtere eventuelle økonomiske konsekvenser (som partene kan påføre hverandre)?		Bilag 5		Kopi
17	Prosjekt	Vil innføring av elektronisk datautveksling mellom etater føre til at øvelser, beredskap, supportavtaler, avtaler for tjenestenivå (SLA)/		Bilag 4		Kopi

		oppetider m.m. må koordineres partene imellom?				
18	Prosjekt	Er rutiner for konfigurasjonsstyring av endringer som påvirker annen part beskrevet? • Er plan for innføring av konfigurasjonsstyring hensiktsmessig for å sikre samhandlingen? • Er ansvar for godkjenning og gjennomføring av endringer plassert hensiktsmessig • Er nødvendige sw utviklingsmiljø, testmiljø og testdata og tilgjengelig for enkelt å håndtere feilretting og videreutvikling? • Er det etablert et forum/samhandlingsforum hvor partene møtes og diskuterer fremtid for samhandlingen. Konfigurasjonsstyring bør gjelde alle typer modeller, operative rutiner for saksbehandling, informasjonsforvaltning, datakvalitet, data-transformasjoner og grensesnitt på alle nivåer og programvare.		Bilag 4, 5 Bilag 6 Bilag 10, Samledokument Bilag 10, Samledokument		Kopi
19	Prosjekt	Er transformasjoner beskrevet og ansvar for vedlikehold og konfigurasjonsstyring av disse hensiktsmessig?		Bilag 5		Kopi
20	Prosjekt	Har partene sikret seg tilgang til hverandres ressurser i aktiviteter og leveranser der dette er nødvendig. Gjelder i de ulike prosjektfaser, utvikling, test og driftsituasjon.		Bilag 4, 11		Kopi

3.2 Utvekslingsavtalen, sjekkliste for Mottaker

Mottakersjekklisten for utvekslingsavtalen forutsetter at Mottaker-sjekklisten for intensjonsavtale er besvart.

Se sjekkliste for avsender og kolonner for Mottaker sjekkliste. For hvert spørsmål i sjekklista er det kommentert om spørsmålet skal snus til å sette mottaker i sentrum eller om spørsmålsteksten kan kopiers som den står.

4 Appendiks: Supplement til sjekklistene

4.1 Beskrivelse av data/opplysningstype

Data bør beskrives i henhold til en 3-lags inndeling med modeller for følgende lag:

- **Begrepsmodell**, som beskriver/definerer hvordan data som utveksles skal tolkes.
    - Denne modellen lages gjerne i UML verktøy eller et ontologiverktøy.
    - Eksempel på metode og verktøy er SERES, evt verktøy som Protegé eller TopBraid.
    - DIFI standard for begrepsbeskrivelser gjelder for dette nivået [6].
    - Opplysningstypene/begrepene som beskrives skal være uttrykt i denne modellen
- **Informasjonsmodell**, som beskriver den sammenhengen de utvekslede data skal tolkes i lyset av.
    - Denne modellen lages gjerne i UML-verktøy eller et ontologiverktøy.
    - Eksempel på metode og verktøy er SERES, evt verktøy som Protegé eller TopBraid.
- **Utvekslingsmodell/meldingsmodell** som beskriver dataformatet som benyttes ved selve utvekslingen. Formatet må evne å koble alle verdier i en gitt utveksling til aktuelle begreper i en begrepsmodell.
    - Denne modellen lages gjerne som et XML Schema eventuelt som et UML klassediagram hvor XML Schema modell kan genereres basert på UML-modellen.
    - Eksempel på metode og verktøy er SERES

Selv for små modeller vil en god editor som bistår med å holde de tre nivåene sammen være til stor nytte. Hver av disse modellene er i bevegelse ved endring av saksbehandlingspraksis, endring i lover og regler. Konfigurasjonsstyring er like viktig for disse modellene som for programkode. Mange prosjekter starter gjerne med å lage modellene i tekstbehandlingsverktøy eller regneark.

For å få med tidsdimensjonen ved informasjonsforvaltning og bruk, kan en stille spørsmål som:

Har det vært eller vil de bli endringer i:

1. Hva data brukes til?
2. Hvordan data tolkes?
3. Hvilke lover og regler som gjelder ved utveksling, forvaltning og bruk av data.
4. Hvordan data innhentes?
5. Hvordan informasjon kobles til annen informasjon?
6. Hvordan data oppbevares, struktureres, formatvalg etc?
7. Datakvalitet eller måten en måler datakvalitet?

Gode begrepsmodellener skal kunne gi svar på bl.a følgende:

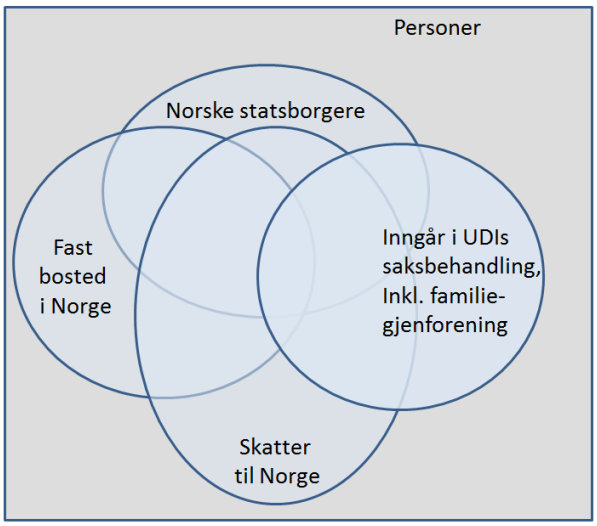
- Hvor kommer begrepene fra, eksempelvis lov, forskrift, praksis etc. Se også bilag 2 til utvekslingsavtalen, hjemmelsgrunnlag.
- Forhold til tilsvarende begrep hos de involverte parter samt juridisk kilde om det finnes. Vurdere om
    - begrepene semantisk ekvivalente
    - begrepene er overlappende, Sub/Super type begreper, Synonyme begreper
    - hvordan transformasjoner av data mellom begreper kan gjøres
- Er avsender og mottaker modellene på samme nivå? Vanlig eksempel på ulikt nivå er hvis begreper hos avsender ikke er begreper hos mottaker, men verdier i en kodeliste i mottakers modell?

Supplerende litteratur kan være:

- Sjekkliste for testing av elektroniske meldinger mellom virksomheter [3]
- ISO 704 Terminologistandardisering [5]
- DIFI standard for begrepsbeskrivelser [6]
- SERES metoder for modellering og kvalitetssikring av modeller [7]
- Livssyklusprosess for utarbeidelse og forvaltning av begrepssystemer [22]
- Standard for begrepskoordinering[23]

4.1.1 Populasjon og endringer i populasjoner

Som del av begrepsmodellen må det også beskrives egenskaper ved populasjonen (hvilke personer/ bedrifter/husstander etc) en har data om. Eksempelvis har SKD oversikt over personer som har en skattemessig relasjon til den norske stat (det vil si en populasjon av personer), mens UDI trenger opplysninger om mange personer som ikke finnes i SKD sine systemer ei heller i folkeregisteret, det vil si UDI trenger informasjon om en deler av de personer SKD har data om, men trenger også data om en rekke andre personer.



Figur 1, sammenheng og ulikhet i populasjoner av personer

Ven-diagrammet over søker å gjenspeile at populasjoner kan overlappe og at en person kan være med i flere populasjoner. Størrelsesforholdet på sirklene gjenspeiler ikke størrelsen på de faktiske populasjonene. For eksempel blir en person norsk statsborger og få fast bosted i Norge. På denne måten vil hvem/hva som inngår i en populasjon være i endring over tid. For elektronisk samhandling er populasjon og endringer i populasjon vesentlig siden samhandling etablerer en type distribuert informasjonssystem som er enklest å forvalte om det er mest mulig stabilt og konsistent over tid. Det hjelper lite å beskrive hvilke data du har i dag og sette opp samhandling basert på et nåtids bilde, for så å oppleve at over tid så endres populasjonen hos deg eller dine partnere slik at forutsetninger for samhandlingen ikke er til stede lengre.

4.2 Prosesser knyttet til etablering, forvaltning og utveksling av data

Prosesser hos avsender og mottaker bør beskrives slik at det er mulig å sette prosessmodellene sammen for å vise grensesnittet i samhandlingen. Vanlig fremgangsmåte vil være først å beskrive aktiviteter og informasjonsutveksling hos avsender og mottaker slik det gjøres per i dag og deretter å beskrive hvordan en ønsker å gjøre det i fremtiden.

Prosessdiagrammer som viser grensesnitt/dataflyt ut av en virksomhet må beskrive hva som gjøres før, under og etter utvekslingen. Hvor en starter å beskrive aktivitetene er et designvalg og må tilpasses det enkelte case og hvor saksbehandling og bruk av data starter. For å forstå diagrammene bør prosessdiagrammet beskrive kriterier for å starte det enkelte prosess-steg samt kriterie for at prosess-steget er ferdigstilt.

- Metodeforslag: En mulig metode og visualisering av samhandling er UML Swimlanes.
- Eksempel på verktøy: Swimlane diagramtype støttes i de aller fleste open source og kommersielle UML verktøy.

Avklaring om hva som skal inkluderes i prosessmodellen og hva som skal beskrives i prosa som tillegg er litt smak og behag, samt avhengig av hvor stor modell en ønsker å visualisere og forvalte.

Spørsmål som bør besvares ved etablering av elektronisk samhandling som angår både prosess, livssyklus for data og informasjonsforvaltning er bl.a.:

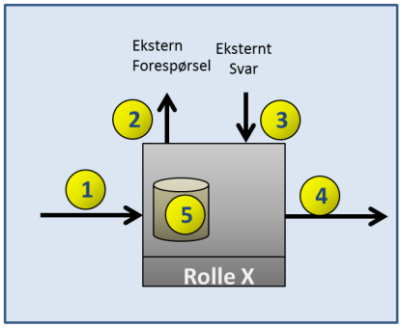
1. Hvor i egen saksbehandlingsprosess produseres data?
2. Hvordan forvaltes data (informasjonsforvaltningsregime)?
3. Er data i en endelig tilstand, eller vil endring/klagebehandling etc. kunne føre til at endringer måtte ettersendes?
4. Ved endring i data, hva er prosessen og kriterier for om data skal ettersendes til dem som har gjort saksbehandling basert på gitte data?
    - Klagebehandling hos avsender, hvor klage tas til følge, skal oppdaterte data ettersende mottaker?
5. Hva er alternative data og tilstander?
6. Finnes historiske data, eller er det kun siste versjon som er aktuell?
    - Kan det være aktuelt å spørre etter data som var gyldige på tidspunkt x, eller ble data endret i løpet av periode a-b?
7. Hva er levetid til data som utleveres, hvor lenge etter utlevering anses de som gode nok for andres saksbehandling?
8. Hva er kriterier for sletting av data?
9. Skal data sendes til deponering hos Riksarkivet iht gjeldende arkivregler for offentlig sektor?

10. Ved lengre verdikjeder av datautveksling arves da plikter og begrensninger fra fler enn kun den som er avsender? Har avsender videresendt data han selv har mottatt og hvor det er knyttet betingelser/begrensninger til data?
11. Hvilke rutiner er beskrevet som sikrer hensiktsmessig varsling av endringer som påvirker mottakers bruk av data? Eksempelvis oppdateringer i prosesser, lover, organisering, datakvalitet etc.

4.3 Kobling mellom aktiviteter og den informasjon som benyttes i aktiviteter

For hver aktivitet bør kobling til informasjon beskrives basert på følgende:

1. Input til aktiviteten fra annen intern aktivitet/hendelse eller tidstrigger.
2. Utveksling med ekstern aktør eller forespørsel om data fra ekstern aktør.
3. Mottak av data fra ekstern aktør, evt. mottak av forespørsel om data.
4. Output fra aktiviteten til intern tilstand/aktivitet.
5. Informasjon som er tilgjengelig for aktiviteten



Figur 2,Informasjon som bindeledd mellom aktiviteter

For hver av informasjonsflytpilene i figuren bør en sikre at en vet:

- kobling mellom aktiviteten og data, og videre til både informasjonsmodell og til begrepsmodell
- kobling mellom aktivitetsmodell med tilhørende dataflyt til jus
- hvilke datakvalitetskriterier som skal oppfylles og vurdering av om disse er tilstrekkelige for saksbehandling og for å oppfylle lovkrav
- hvilke sikkerhetsmessige aspekter som skal oppfylles og vurdering av om disse er tilstrekkelige for saksbehandling og for å oppfylle lovkrav
- hvordan feilhåndtering i saksbehandling, dataflyt, datakvalitet, teknisk system m.m. skal utføres.

4.4 Jus

Følgende er sentrale betraktninger knyttet til juss, se også innholdet i utvekslingsavtalen som er en mer komplett opplisting av juridiske momenter.

Juss hos avgiver: Avgivers materielle regler definerer begrepene/opplysningstypene. Avgiver må derfor definere sine begreper grundig. Dersom dette er juridiske begreper, så vil definisjonen være en rettslig definisjon, og den vil være basert på kilder (rettskildefaktorer). Tolkningen kan og skal dokumenteres.

Disse definisjonene definerer opplysningstypene, og gir forståelsen av opplysningene/data/verdiene.

For at mottaker skal forstå verdiene av begrepene, er det nødvendig at avgiver forklarer den saksbehandlingen som leder til fastsettelsen av verdiene/opplysningene/dataene.

Juss hos mottaker er de rettslige grunnlag som inneholder vilkår for materielle avgjørelser som hører under mottakers personelle kompetanse/ansvarsområde. Vilkårene er i hovedsak formulert i lov og forskrift. Disse formulerte vilkårene er bare utgangspunktet for fastsettelsen av innholdet i vilkårene. Det er innholdet i vilkårene som definerer mottakers opplysningstyper, altså hvilke opplysningstyper som er relevante for mottaker. Innholdet i vilkårene må derfor fastsettes. Dette gjøres ved en prosess som kalles juridisk metode, og som er styrt av rettskildeprinsipper. Fastsettelsen av innholdet i vilkårene, og dermed hvilke opplysningstyper som er relevante kan enten gjøres generelt eller konkret. Det mest hensiktsmessige er her at mottaker gjør dette konkret, som altså innebærer at mottaker tar standpunkt til om de opplysningene avgiver har er relevante under vilkårene. (Alternativt kan mottaker ta standpunkt til om enkelte elementer/kriterier i avgivers opplysningstyper er relevante.) Det er ikke særlig hensiktsmessig at mottaker tar generelt standpunkt til hvilke andre opplysningstyper som er relevante, abstrahert fra de konkrete opplysningstypene avgiver kan gi.

Resultatet må beskrives på en måte som er forståelig for de som skal lese dette, altså både jurister og teknologer? Dette er jurister hos mottaker og avgiver, og teknologer hos avgiver og mottaker. For at mottaker skal kunne ta standpunkt til om avgivers opplysningstyper er relevante, så forutsetter det at mottaker forstår avgivers opplysningstyper. Skinn enighet og skinn uenighet må oppklares, og det må verifiseres.

Dersom avgivers opplysninger umiddelbart er relevante for mottaker i henhold til dette, så kan utveksling skje uten videre.

Dersom det må gjøres noe med avgivers begreper/opplysninger, så kan de likevel utveksles, men kan ikke brukes hos mottaker uten tilpasninger/transformasjon.

Juss hos mottaker: Mottaker plikter å kvalitetssikre de opplysningstypene og opplysningene de får fra avgiver, og kan ikke benytte opplysningene i egen saksbehandling uten at de er tilstrekkelig sikre på at opplysningene er korrekte, og at de forstår opplysningenes innhold, jf forvaltningsloven § 17?

Dette medfører også at mottaker har en viss plikt å kontrollere avsenders organisasjon for opplysningsinnhenting/opplysningsfastsettelse. Dette gjelder særlig dersom beviskravene er forskjellige på avsendersiden og mottakersiden, og de opplysningene som utveksles er faktaopplysninger. Dersom avsenders opplysninger er opplysninger om innholdet i vedtak hos avsender, så må dette som utgangspunkt tolkes slik at opplysningene er tilstrekkelig gode. Spørsmålet om opplysningene er blitt forfeilet fra vedtak til oversendelse, er et annet spørsmål. Det er åpenbart at det ikke må skje, og at mottaker må kontrollere at avsenders system sikrer at dette ikke skjer. Hvordan dette skal sikres er ikke et rettslig spørsmål.

Juss som ramme: avgiver må forsikre seg om at de har rettslig anledning til å utlevere opplysningene til mottaker. Det beror på en tolkning og anvendelse av alle reglene om taushetsplikt hos avgiver og innhentingshjemmel hos mottaker.

Dersom avgiver bare kan utlevere opplysninger som er «nødvendige» i mottakers saksbehandling, (og slik vil innhentingshjemlene vanligvis måtte forstås enten det står uttrykkelig eller ikke), så innebærer det at mottaker må redegjøre for tolkningen av vilkårene i de materielle hjemlene (som altså må vise at avsenders opplysninger er relevante for mottakers saksbehandling) slik at avgiver kan se at opplysningene er «nødvendige».

Juss hos mottaker: I relasjon til personopplysningslovens behandlingsansvar, så blir mottaker behandlingsansvarlig for opplysningene ved overlevering, og dette betyr antakelig at avsender ikke har noe rettslig plikt til å kontrollere hvordan mottaker benytter opplysningene. Unntak kan nok tenkes for enkelte typer opplysninger og i relasjon til enkelte persongrupper.

Relevante spørsmål kan være:

1. Har vi hjemmel for å be om data fra annen etat?
2. Er det krav til levetid for data?
3. Hvordan skal sletting håndteres?
4. Fletting / kobling av registre, er det problematisk?
5. Er det krav til oppdatering, omgjøringsplikt mm.
6. Hva er krav til integritet?
7. Hva er krav til konfidensialitet?
8. Hva er krav til sporbarhet?
9. Hvor kommer data fra, har din avsender også mottatt data fra en annen avsender/borger/næringsdrivende?
10. Hvem/hvilke rolle har og har hatt innsyn til data? (tilgang og aksessrettigheter)
11. Hvem planlegger å benytte de aktuelle data videre og til hva?

Vanlige lover og regler som kan gjelde for informasjonsoppbevaring, utveksling, åpenhet, sletting, kobling av informasjon er:

1. Personopplysningsloven
2. Offentlighetsloven
3. Arkivloven
4. Regnskap og revisjonslovgivning
5. Sikkerhetsinstrukser

4.5 Transformasjoner

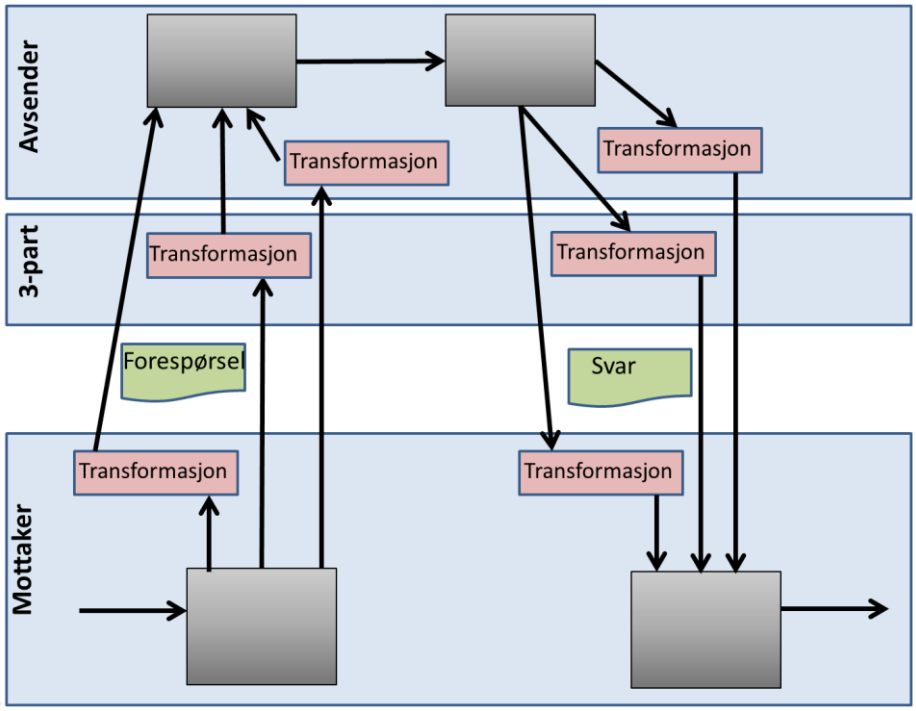
Når en sender en forespørsel om data til annen etat og får svar i henhold til forespørsel skjer det en rekke transformasjoner. Eksempler på transformasjoner er:

- Bæreprotokoll, selve utvekslingsmekanismen på et lavere teknisk nivå.
- Sikkerhetsmekanismer hvor kombinasjoner mellom kanalsikkerhet, meldingssikkerhet og skallsikkerhet/sikre soner og applikasjon med autentisering og autorisasjonsstyring benyttes.
- Formatkonvertering, mellom formater som for eksempel: eksportformat for database, XML, CSV, EDIFACT, RDF, proprietære format osv.
- Modellkonvertering, transformerer data i et gitt format til å være i overensstemmelse med en annen informasjonsmodell enn kilde.
    - Attributt-tilpasninger. Eksempelvis, om et avsender system skiller på fornavn, mellomnavn og etternavn, vil data kunne konverteres presist til en modell for fornavn + etternavn hvor mellomnavn er siste del av fornavnet. Motsatt vei går ikke,

dermed er dette en transformasjon med tap i presisjon, dvs. hva som er mellomnavn blir vanskelig å finne ut i data som er i henhold til modellen hos mottaker.

- Begrepskonvertering, er mulig i en del tilfeller der sammenhenger mellom begreper er tydelig beskrevet.
    - Eksempel: avsender kan ha mer presise begreper enn mottaker. Det åpner for muligheten til at alle data som er i henhold til avsenders begrep også vil være innenfor definisjonen av mottakers begrep. Konkretisert: Om avsenders begrep for personinntekt per år (iht et gitt regelverk) er mer presist enn mottakers tilsvarende personinntekt per år begrep, vil mottaker trolig kunne benytte data som er i henhold til avsenders begrepsmodell. Motsatt trenger ikke være tilfelle, det må utredes om er mulig.
    - Eksempel på endring av benevnelse/type: en kan for mange formål omforme opplysninger som er oppgitt per år til et gjennomsnitt per mnd. Om en da spør på inntekt for juni 2012 må mottaker vite at svaret er et gjennomsnitt og ikke faktisk verdi.
- Populasjonstilpasninger. Elektronisk samhandling utfordrer offentlig sektor i retning av å se på seg selv som forvalter av et stort distribuert informasjonssystem. Ulike offentlige registre og saksbehandlingssystemer vil ha data om ulike deler av befolkningen, bilparken, næringslivet etc. Det må derfor avklares hva fravær av data om et objekt i et system egentlig betyr og hva som skal gjøres om et spørsmål ikke returnerer et svar.

Som figuren under viser to hovedtidspunkt for transformasjon, det er ved spørring og ved svar.



Figur 3, Transformasjoner av data, vanlige alternativer

Den som spør kan lage en forespørsel basert på sin informasjons- og begrepsmodell og transformere spørringen til modeller hos den som skal avgi informasjon. Alternativt kan tredjepart eller avsender

gjøre transformasjon av spørringen. Når svaret på forespørselen lages kan avsender transformere til mottakers modell, evt. tredjepart eller mottaker kan selv gjøre transformasjonen.

I praksis blir det ofte transformasjoner både ved spørring og ved svarhåndtering. Disse transformasjonene er kritiske for at utvekslingen skal fungere i henhold til hensikt.

I forbindelse med transformasjon endres gjerne data mellom eksakte verdier ⇔Terskel verdier (Over/Under terskel) ⇔Ja/Nei – True/False. Disse ulike typer svar kan i noen tilfeller håndteres på ulike måter sikkerhetsmessig siden de kan ha ulik krav til konfidensialitet.

Det er sentralt at mottaker har tilstrekkelig forståelse for saksbehandlingen bak dataene (hvordan verdiene har fremkommet) både internt hos avsender, men også hva som skjer med data i transformasjonene.

4.6 Risikostyring, kvalitetssystemer og gevinstrealisering

Det er sentralt at deltakerne ser forskjell på et samhandlingsprosjekt og et etatsinternt prosjekt.

> Et bilde kan være forskjellen på en enkelt fotballspiller som har individuelle ferdigheter versus fotball-lagets kollektive ferdigheter. Treneren skal hjelpe både på det individuelle og det kollektive plan. Tilsvarende må samhandlingsprosjekter ha en trener eller coach og risikostyring og kvalitetssikring må fokusere på både individuelt nivå og kollektivt nivå. Suksessen er et resultat av lagets kollektive prestasjoner.

Tre tilnærminger til måloppnåelse er (1) risikostyring, (2) helhetlig kvalitetssystem og (3) gevinstrealisering. Disse tre bør ved elektronisk samhandling sees i sammenheng og avsender og mottaker har gjerne ulike tradisjoner for hvilken tilnærming de legger mest vekt på i prosjektgjennomføring og i organisasjons-forbedringsprogrammer. Fokus må endres fra å være etatsinternt til å fokusere på kollektive mål, nå skal etatene sikre gevinster basert på esamhandling og de må spille hverandre god. Kulturmessig vil fokus på kollektiv måloppnåelse by på endring og utfordringer.

Flere av elementene som er sentrale i gevinstrealisering er også sentrale i de andre måtene å strukturere "prosjekter" på. Vi anbefaler at etatene ser disse tre som supplerende til hverandre men også overlappende. Utfordringen for etatene blir å kombinere de ulike tilnærmingene. Sjekklista utfordrer etatene til å ta stilling til hvordan de tre tilnærmingene er tenkt benyttet. Ved å bruke risikotilnærming for gevinstrealisering, dvs at en gevinst som kanskje ikke oppnås er en risiko, da kan en benytte risikometoder med tiltak også for å sikre gevinstrealisering. Se mer om gevinstrealisering i kapittel gevinstrealisering, 4.8.

Vi anbefaler å se de tre hovedspørsmålene under samlet for å sikre at hovedmål, leveranser og gevinster skal være godt egnet og kunne realiseres.

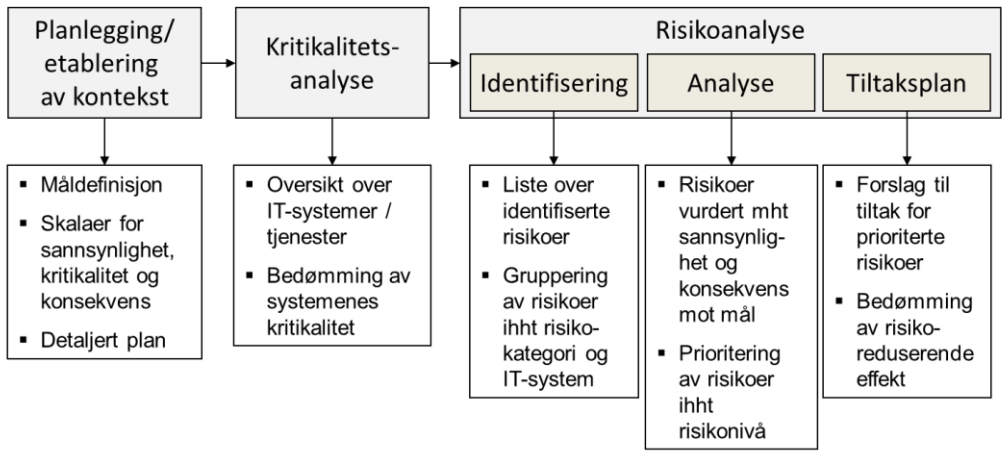
11	Risikostyring	Er metodisk tilnærming og tidsplan for risikoanalyser avklart?
12	Risikostyring	Er metodisk tilnærming og tidsplan for kvalitetsstyring avklart?
13	Risikostyring	Er metodisk tilnærming og tidsplan for gevinstrealisering avklart?

DIFIs maler og arbeid med risikostyring fokuserer primært på informasjonssikkerhet, men i beskrivelse av motivasjon viser DIFI overordnet forståelse for hva potensialet ved god risikostyring kan bety for virksomheter. DIFIs formuleringer i veilederen [21] er som følger:

Kunnskap om risiko- og mulighetsbildet

God informasjonssikkerhet forutsetter kunnskap om risiko- og mulighetsbildet. For å kunne prioritere riktig og begrunne sine valg, eventuelt manglende valg, av sikkerhetstiltak, må virksomheten først ha oversikt over egne oppgaver og verdier, hvilke regler som gjelder og hvilken trussel og risiko de står overfor. Sikkerhetstiltak kan avverge og forebygge trusler, men også gjøre løsninger mulig som ikke ellers ville vært gjennomførbare.

I Semicolons tilnærming vil en i analysefasen se på samhandlingen som et distribuert informasjonssystem. Risiko som hindrer god endring og gevinstrealisering er primærfokus ved Semicolons risikotilnærming. Vanlig fremgangsmåte for å gjennomføre en risikoanalyse er illustrert i figuren under. DIFIs veileder for risikoanalyse med fokus på informasjonssikkerhet er kun en av flere delanalyser.



Figur 4, Vanlige aktiviteter i en risikoanalyse

Under planlegging skal en definere hva en ønsker å måle risiko opp mot. Kategorier av risikoer innen informasjonssikkerhet og IKT er vanligvis:

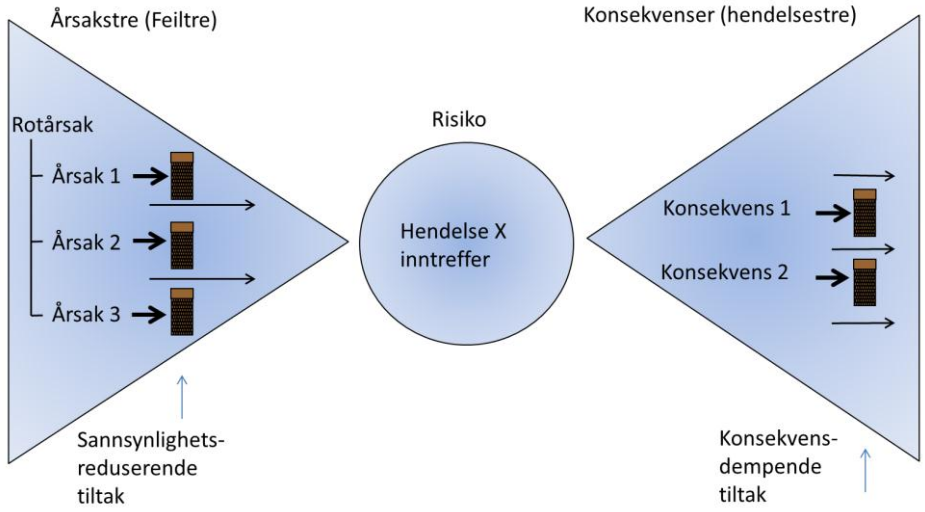
- Konfidensialitet
- Integritet
- Tilgjengelighet

Ved etablering av elektronisk samhandling vil det være hensiktsmessig å supplere med ytterligere dimensjoner som:

- Oppnåelse av
    - prosjektmål 1
    - prosjektmål 2
    - …
- Økonomi
- Omdømme
- Endringsevne
- Levetid av system (SW/HW)

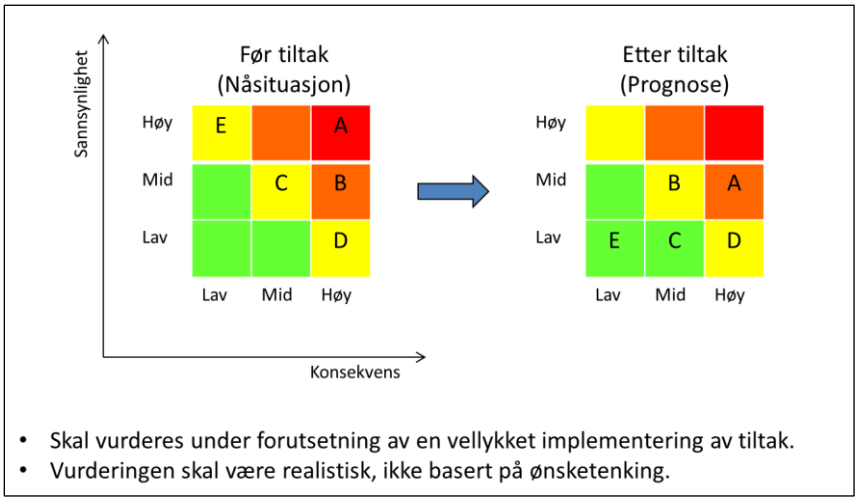
Ved å benytte risikomål ut over de vanlige informasjonssikkerhetsmålene endrer vi risikoanalysen fra å være avgrenset til informasjonssikkerhet til å omfatte mål for prosjektet og virksomhetene.

Når risikoer er identifisert og sannsynlighet og konsekvens vurdert gjennomføres identifisering og systematisering av tiltak. Hensikten med tiltakene er å redusere risiko og vanligvis vil tiltak føre til enten redusert sannsynlighet eller redusert konsekvens. Figuren under viser forskjellen på tiltak som har til hensikt å redusere sannsynligheten for at en risiko inntreffer, versus tiltak som har til hensikt å redusere konsekvens ved at en risiko har inntruffet.



Figur 5, sløyfe, BowTie figur for tiltak

Ved bruk av sjekklistene bør mengden risiko i et prosjekt allerede være godt redusert, men ved gjennomføring av en risikoanalyse vil en få klarlagt restrisikoen avsender og mottaker er eksponert for. Enkelte risiko vil kun gjelde avsender eller mottaker, og derfor bør de involverte kjøre selvstendige risikoanalyser. Det kan oppstå situasjoner hvor en risiko hos avsender kan være positivt for mottaker, dette er typisk tilfelle når endring i samhandling fører til at risiko flytter seg fra en part til en annen.



Figur 6, Risikonivå før og etter vellykket tiltak

De enkelte risiko og tiltak plasseres hos en ansvarlig rolle evt person.

Når risikoanalysen er ferdig går man over en fase med risikostyring. Da gjelder rutiner for å fange opp risiko som oppstår ved ulike typer endringer og hendelser. Ansvarlig for risikostyringen må sørge for at risikobildet oppdateres med jevne mellomrom.

Supplerende litteratur kan være:

- Risikovurdering - en veiledning til Rammeverket for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor. DIFI [20]
- Risikoanalyse, KITH [21]

4.7 Kvalitet på data

Kjent og tilstrekkelig datakvalitet er en viktig forutsetning for elektronisk samhandling og spesielt viktig ved automatisering av informasjonsbehandlingen og saksbehandlingsbeslutninger basert på utvekslet informasjon. Ved samhandling er det sentralt for partene å erkjenne at det som er tilstrekkelig datakvalitet for et bruksområde ikke trenger å være tilstrekkelig for andre. Måling og forbedring av datakvalitet er et kontinuerlig arbeid som krever metoder, ressurser, verktøy og styring. Det er per i dag godt etablerte standarder for datakvalitet som er velegnet for et mangfold av bruks scenarier.

Datakvalitet er i seg selv en show-stopper for å etablere elektronisk samhandling. Uten tilstrekkelig kvalitet på data som mottas kan data heller ikke benyttes til saksbehandling. For å unngå show-stopper situasjoner er det viktig at alle prosesser knyttet til datakvalitet er godt beskrevet, at all input-data er kvalitetssikret og at det finnes en beskrivelse for hvilket kvalitetsregime disse data har fulgt.

Supplerende spørsmål rundt datakvalitet kan være:

1. Er data av en kvalitet som gjør at organisasjonen kan avgi dem uten avtaleklausuler om mulige feil og mangler?
2. Er prosesser for å sikre datakvalitet beskrevet? Eksempler på prosesser kan være:
    a. Sikring av datakvalitet ved mottak/innhenting?
    b. Sikring av datakvalitet ved fletting av datakilder
    c. «Vasking» av data mot for eksempel andre kilder?
    d. Periodiske analyser for å sjekke status og utviklingstrender for datakvalitet.
    e. Kontrollere data mot andre kilder for å identifisere evt avvik/forskjeller. Gjøres dette kun på utvalg av data eller for alle data som mottas, benyttes?
3. Er kvalitetsnivåer definert?
4. Er analyser av datakvalitet gjort på de data som skal utveksles?
5. Bør avsender stille krav til datakvalitet i datakilder hos mottaker før avsenders data benyttes hos mottaker?
6. Hvordan påvirker transformasjoner datakvalitet?
7. Har avsender og mottaker konkrete krav til datakvalitetsnivå beskrevet i for eksempel i henhold til ISO 8000?
8. Hvor lav datakvalitet kan avsender utlevere uten å varsle mottaker?
9. Hvordan er datakvalitetsprosess og datakvalitetskrav hos avsender og mottaker harmonisert?
10. Utveksles tilstrekkelig med livsløpsinformasjon sammen med de data som utveksles (Provenance informasjon)? Sagt på annen måte, utveksles data sammen med beskrivelse av opphav og livssyklusstatus, eller vet mottaker på annen måte hva som er opphav og livssyklusstatus på data? [9]

Målbare datakvalitetskrav som er koblet til både datakvalitetsprosesser og selve data bør med i utvekslingsavtalen eller relevante bilag.

Ved elektronisk samhandling oppstår den situasjon av virksomheter blir avhengig av hverandres informasjon. En måte å systematisere utfordringer på er å ta utgangspunkt i datakvalitet. Under er en liste med ti rot-kildeproblemer til datakvalitet som alle vil være til stede i mer eller mindre grad ved elektronisk samhandling.

Ti rot-kilder til datakvalitetsproblemer er i følge Journey to Data Quality [16 s80]:

1. *Multiple Data Sources.*
   - *Multiple sources of the same information produce different values for this information. This can include values that were accurate at a given point in time.*
2. *Subjective Judgement in data production*
   - *Information production using subjective judgment can result in the production of biased information.*
3. *Limited computing resources*
   - *Lack of sufficient computing resources limits accessibility to relevant information.*
4. *Security/accessibility trade off:*
   - *Easy access to information may conflict with requirements for security, privacy, and confidentiality.*
5. *Coded data across disciplines:*
   - *Coded data from different functions and disciplines is difficult to decipher and understand. Also codes may conflict.*
6. *Complex data representations:*
   - *Algorithms are not available for automated content analysis across instances of text and image information. Non-numeric information can be difficult to index in a way that permits location of relevant information.*
7. *Volume of data.*
   - *Large volumes of stored information make it difficult to access needed information in a reasonable time.*
8. *Input rules too restrictive or bypassed.*
   - *Input rules that are too restrictive may impose unnecessary controls on data input and lose data that has important meaning. Data entry clerks may skip entering data into a field (missing information) or arbitrarily change a value to conform to rules and pass an edit check (erroneous information)*
9. *Changing data needs.*
   - *As information consumers' tasks and the organization environment (such as new market, new legal requirements, new trends) change, the information that is relevant and useful changes.*
10. *Distributed heterogeneous systems.*
    - Distributed heterogeneous systems without proper integration mechanisms lead to inconsistent definitions, formats, rules, and values. The original meaning of data may be lost or distorted as data flows and is retrieved from a different system, time, place data consumer, for same or different purpose.

Supplerende litteratur kan være:

- ISO 8000 Data Quality [10]

- Journey to Data Quality [16]
- Data Quality. [17]

4.8 Gevinstrealisering

Bevisst holdning til gevinstrealisering øker sjansene for at potensiell nytte (gevinst) identifiseres tidlig og at identifisert nytte faktisk realiseres. Gevinstrealisering handler i kort fortalt om tre ting:

- Etablere gode (og omforente) mål
  - konkretiseres på et slikt nivå at det er klart beskrevet hvilke nytte (gevinst) som forventes og i hvilket omfang.
- Etablere (gevinstrealiserings)plan med tiltak for å håndtere risiko og nå målene
  - dette overlapper med tidligere beskrevne tiltak for å redusere risiko, men kan også gå utover en vanlig risiko-tilnærming om at risiko fokuserer på å unngå nedsiden/tap. Risikostyring kan benyttes for å styrke mulighetene. Planen skal også inneholde informasjon om hvordan målinger skal gjennomføres og dermed legge godt grunnlag for målinger (underveis og når gevinstene forventes realisert). På samme måte som med risiko anses det som viktig å etablere ansvar for ulike tiltak og når de enkelte gevinstene forventes realisert.
- Oppfølging, måling og evaluering
  - gevinstrealiseringsplanen danner grunnlag for oppfølging av tiltak og planlagte gevinster. Endringsledelse er sentralt i oppfølgingen. Målinger gjennomføres som spesifisert i gevinstrealiseringsplanen. Det er regnet som god praksis å evaluere måloppnåelse og vurdere grunnlag for eventuelle nye muligheter som har oppstått som følge av arbeidet som er gjort.

Det er viktig at punkt 1 og 2 adresseres tidlig i et prosjekt siden disse legger grunnlag for oppfølging og endelig realisering av gevinster.

4.9 Håndtering av endring av opplysninger, klagebehandling og omgjøring

Ved bruk av informasjon fra avsender og hvor informasjonen kan endres etter at den er benyttet i saksbehandling må det avklares hva som skal gjøres om data hos avsender/kilden endres. Hovedutfordringen er klagebehandling kombinert med omgjøringsplikt.

Punkter som kan være relevant å avklare i denne sammenheng kan være:

- Push eller pullmodell av data og påbegynte klager.
  - Skal avsender logge hvem de har oversendt data om og ettersende innen kjente frister?
  - Skal mottaker sende forespørsel på alle vedtak siste x mnd og spørre om noen av disse har klaget og hva klagen førte til.
- Er det behov for å harmonisere klagefrister?
  - Eksempel, en borger klager på SKD ligning og får medhold, dette fører til at søker kommer over terskelverdi for å få oppholdstillatelser hos UDI. UDI vedtak skal egentlig endres, men klagefrist hos UDI kan være utgått før SKD har ferdigbehandlet klagen. Sett fra borgers ståsted er dette en veldig uheldig situasjon.

Skal trigger for å informere annen etat om endring være at:

- Borger har sendt klage?
- Konklusjon på klage foreligger og klagen førte til endring?
- Avsender skal uansett sende info om at de har kontrollert behovet for ettersending, men at ingen saker hadde behov for å få ettersendt data.

4.10 Sikkerhet

Etablering av ulike typer sikkerhetsmekanismer er en forutsetning for etablering av elektroniske samhandling. Eksempler på spørsmål knyttet til om tilfredsstillende sikkerhetsmekanismer og rutiner er tatt i bruk for å tilfredsstille lovkrav i forbindelse med:

1. Mottak av data
2. Forvaltning og sletting av data
3. Avgivelse av data
4. Anonymisering av data
5. Rapportering og statistikk
6. Ved omorganisering eller endring av ansvar og arbeidsoppgaver

For hvert av punktene over vil vanlige tema innen datasikkerhet være:

- Konfidensialitet: Å sikre at informasjon bare er tilgjengelig for de som skal ha tilgang.
- Integritet: Å sikre at informasjon er korrekt og fullstendig.
- Tilgjengelig: Å sikre at informasjon er tilgjengelig innenfor de krav som er satt.
- Sporbarhet og ikke-benekting (Engelsk: Non repudiation): Beskriver metoder som skal dokumentere at en handling (på informasjon) virkelig har vært gjort av en konkret definert person/system.
- Autentisering: å autentisere en person kan bety å kontrollere vedkommendes identitet/elektroniske ID eventuelt ID til et system som representerer en person eller rolle.

Se gjerne:

- [1] ISO/IEC 27010 — Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications.

4.11 Budsjett og planlegging

Tbd

4.12 Krav til gjennomføring av selve utvekslingen

Tbd, men bl.a.

Punkter som bør være med i kravlisten er bl.a.:

- Tilgjengelighet på teknisk bistand hos avsender evt tredjeparter
- Tekniske responstider og kapasitetsvolum
- Bruk av sikkerhetsmekanismer, rutiner og bruk av protokoller
- Krav til rutiner og teknisk støtte ved ulike typer feilhåndtering

5 Appendix: Begreper benyttet i dokumentet

Tbd

6 Appendix: Referanser

1. ISO/IEC 27010 — Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications.
    - http://www.iso27001security.com/html/27010.html
2. Sjekkliste for informasjonssikkerhet i kraftforsyninen
    - http://www.nve.no/Global/Sikkerhet%20og%20tilsyn/Kraftforsyningsberedskap/Sjekkliste%20for%20informasjonssikkerhet%20i%20kraftforsyningen.pdf
3. Sjekkliste for testing av elektroniske meldinger mellom virksomheter, September 2010. Nasjonalt meldingsløft. Helsedirektoratet.
    - http://www.helsedirektoratet.no/publikasjoner/sjekkliste-for-testing-av-elektroniske-meldinger-mellom-virksomheter/Sider/default.aspx
4. NIEM user guide, se primært side 58-68
    - http://reference.niem.gov/niem/guidance/user-guide/vol1/
5. ISO 704, Terminology work -- Principles and methods/ NS-ISO 704 – terminologistandardisering på norsk
    - http://www.sprakrad.no/nb-NO/Toppmeny/Publikasjoner/Spraaknytt/Spraknytt-12011/NS-ISO-704/
6. DIFI standard for begrepsbeskrivelser
    - http://www.standard.difi.no/filearchive/2012-02-02-mal-begrepsbeskrivelser-0-9.pdf
7. Konseptskisse SERES, Brønnøysundregistrene, juni 2008.
    - http://www.brreg.no/samordning/semantikk/SERES_konseptskisse_v1_0.pdf
8. NIEM quality assurance strategy and plan. 20. Mai 2008.
    - http://reference.niem.gov/niem/guidance/quality-assurance-strategy-and-plan/1.0/quality-assurance-strategy-and-plan-1.0.pdf
9. Provenance interchange working group charter
    - http://www.w3.org/2011/01/prov-wg-charter.html
10. ISO 8000 Data Quality
    - http://en.wikipedia.org/wiki/ISO_8000
11. Issues and guidance for opening governmental judicial research data. Anneke Zuiderwijk et al. EGOV 2012.
12. Semicolon: Veiledning i bruk av maler og sjekklister. 18. desember 2012, versjon 1.0. Thom-Kåre Granli (Institutt for Privat rett, UIO), Terje Grimstad (Karde), Per Myrseth (DNVKEMA) og Erlend Øverby (Karde).
13. Veiledning i bruk av avtaler med bilag, Thom-Kåre Granli.
14. Intensjonsavtale om elektronisk utveksling av opplysninger. Versjon 0.3, Desember 2012. Thom-Kåre Granli
15. Avtale om elektronisk utveksling av opplysninger, med bilag. Versjon 3.2. November 2012. Thom-Kåre Granli.

16. Journey to Data Quality. Yang W. Lee, Leo L. Pipino, Richard Y. Wang, James D. Funk. The IT press, 2006.
17. Data Quality. Consepts, Methodologies and Techniques. Carlo Batini and Monica Scannapieco. Springer 2006.
18. Arkitekturprinsipper Difi versjon 1.0 Side 1 av 8 03.04.2009
19. Overordnede IKT-arkitekturprinsipper for offentlig sector. DIFI, 3. April 2009. http://www.difi.no/filearchive/ikt-arkitekturprinsipper_bhnq1.pdf
20. Risikovurdering - en veiledning til Rammeverket for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sector. DIFI, januar 2010. http://www.difi.no/filearchive/rapport-veiledning-til-rammverket-versjon-0-1.pdf
21. Risikoanalyse. Metodegrunnlag og bakgrunnsinformasjon. KITH Rapport 13/2000. http://www.kith.no/upload/995/R13-00Risikoanalyse-v1.pdf
22. Livssyklusprosess for utarbeidelse og forvaltning av begrepssystemer. Februar 2011, Versjon 1.0. Vibeke Dalberg, DNV; Per Myrseth, DNV; Jim Yang, KITH. http://www.semicolon.no/Rapport_prosess_begrepssystem_Final.pdf
23. Standard for begrepskoordinering. DIFI. Versjon/dato: 0.8 / 2012-10-21