

**Grunddataprogrammet under den
Fællesoffentlige Digitaliseringsstrategi 2012 – 2015**

Delprogram 2: Effektiv genbrug af grunddata om adresser,
administrative inddelinger og stednavne

Adresseprogrammet - Målarkitektur Bilag D - Arkitekturrammer

MBBL-REF: 2012-3566

Version: 2.0

Status: Godkendt

Dato: 19. maj 2015

Dokument historie

Version	Dato	Beskrivelse	Initialer
0.8	26.03.2013	Grundskabelon oprettet som kopi af tilsvarende dokument fra GD1. Punkter uden relevans for GD2 er fjernet.	S&D KFC
0.9	11.04.2013	Tilretning ifht. kommentarer modtaget på afsluttende workshop onsdag d. 10/4-13.	S&D KFC
0.9a	14.04.2013	Enkelte tilføjelser i afsnit 3.3 og 3.5	MBBL MLI
1.0	25.04.2013	Godkendt af GD2 styregruppe	MBBL MLI
1.8	07.05.2015	Udkast til en version 2.0 af målarkitekturen med tilpasninger i henhold til erfaringer fra arbejdet med løsningsarkitekturer samt de fælles arkitekturrammer vedtaget i Grunddataprogrammet juni 2014.	S&D KH
2.0	19.05.2015	Godkendt af styregruppen	MBBL THJ

Indholdsfortegnelse

1. INDLEDNING.....	4
1.1 DOKUMENTETS FORMÅL	4
1.2 METODE	4
1.3 PROCES	4
1.4 LÆSEVEJLEDNING	5
2. FÆLLES ARKITEKTURRAMMER	6
2.1 VILKÅR OG RAMMER	6
2.2 ANVENDELSE AF ARKITEKTURRAMMER	6
2.3 VIDEREUDVIKLING AF ARKITEKTURRAMMER	6
3. Udstilling af Grunddata	7
3.1 SERVICES – Udstilling og anvendelse	7
3.2 SERVICES – Navngivning og formater	7
3.3 METADATA.....	8
3.4 HISTORIK OG NØGLER.....	9
3.5 DOKUMENTATIONSKRAV.....	9
3.6 ANSVAR FOR SERVICES.....	9
4. GRUNDDATA - GENERELLE EGENSKABER.....	10
4.1 TIDSMÆSSIGE EGENSKABER - DOBBELTHISTORIK	10
5. HÆNDELSER OG FEJLMELDING.....	11
5.1 HÆNDELSER.....	11
5.1.1 Anvendelse af hændelsesbeskeder	11
5.1.2 Definition af hændelsesbeskeder	11
5.1.3 Generering og udstilling af hændelsesbeskeder	11
5.2 FEJLMELDING	12
6. SIKKERHED	13
6.1 KRAV TIL SIKKERHED	13
6.2 SIKKERHEDSKONCEPT	13
6.3 BRUGERE OG BRUGERROLLER	14

1. Indledning

1.1 Dokumentets formål

Dokumentet har til formål at fastholde og dokumentere forskellige vilkår og arkitekturrammer for adressedataprogrammet. Nogle af disse bygger på fællesoffentlige standarder og anbefalinger, mens andre er antagelser, som adressedataprogrammet har været nødt til selv at fastlægge.

Derudover indeholder dokumentet en liste over adressedataprogrammets forskellige forretnings- og it-principper, dvs. principper som skal være styrende i kravspecificering hhv. udvikling af it-løsninger inden for adressedataprogrammet.

Dokumentet er et bilag til dokumentet "GD2 – Målarkitektur".

1.2 Metode

Arkitekturrammerne fastlægges dels gennem dialog med grunddataprogrammet som helhed hhv. delprogram 7 omkring den fælles offentlige datafordeler.

I det omfang grunddataprogrammet har påtaget sig opgaven med at udstikke fælles retningslinier og standarder, tages disse til efterretning i delprogrammet. For øvrige områder fastlægges de nødvendige standarder internt i delprogrammet i et samarbejde med delprogram 1 – Ejendomsdata.

1.3 Proces

De fælles arkitekturrammer er opsamlet ifb. arbejdet med systemer, begreber og processer i hhv. Ejendomsdataprogrammet (GD1) og Adresseprogrammet (GD2).

Derudover har der specifikt været nedenstående proces ifb. målarkitekturdokumentet:

- Sammenskrivning af de forskellige arkitekturmæssige afklaringspunkter i et "Grunddata – Arkitekturspørgsmål" dokument, som blev sendt til grunddata programmets sekretariat.
- Afholdelse af møde 18. februar 2013 mellem Ejendomsdataprogrammet, Adresseprogrammet og Datafordeler programmet (GD7). Gennemgang af de forskellige arkitekturspørgsmål med et første bud på besvarelse af disse.
- Modtagelse af skriftlig besvarelse 15. marts 2013 fra grunddataprogrammet ift. de forskellige arkitekturspørgsmål.
- Afholdelse af 1. målarkitektur workshop den 19. marts 2013. Her blev grunddataprogrammets tilbagemeldinger på de stillede arkitekturspørgsmål gennemgået og vurderet.
- Sammenskrivning og udsendelse til skriftlig kvalitetssikring. Kommentarer fra workshop indarbejdet og dokumentet udsendt 2. april 2013 til afsluttende skriftlig kvalitetssikring i sammenhæng med målarkitektur dokumentet.

I 2. kvartal 2014 blev der i et samarbejde mellem Ejendomsdataprogrammet, Adresseprogrammet, Datafordelerprogrammet og Digitaliseringsstyrelsen etableret en proces

med detaljering af de forskellige rammer. Dette resulterede i, at Grunddataprogrammet juni 2014 godkendte et sæt arkitekturrammer bestående af et covernotat samt 16 underbilag.

Målarkitekturens arkitekturrammer er med udgangspunkt i dette fælles grundlag, erfaringer fra arbejdet med løsningsarkitekturer mv. opdateret maj 2015.

1.4 Læsevejledning

Udover dette indledende kapitel indeholder dokumentet følgende kapitler:

- **Kapitel 2 – Fælles arkitekturrammer**
Indeholder en beskrivelse af hvorledes de fælles arkitekturrammer skal anvendes og videreudvikles.
- **Kapitel 3 – Udstilling af grunddata**
Indeholder rammer for udstilling, anvendelse og navngivning af grunddataservices – herunder regler ift. metadata, historik, dokumentation samt ansvarsplacering ift. specifikation og udvikling af services.
- **Kapitel 4 – Grunddata – generelle egenskaber**
Indeholder generelle krav til grunddata ift. brug af nøgler og tidsmæssige egenskaber.
- **Kapitel 5 – Hændelser og fejlmelding**
Indeholder en beskrivelse af rammer i relation til hhv. anvendelse af hændelser og understøttelse af fejlmeldinger ift. grunddata.
- **Kapitel 6 – Sikkerhed**
Indeholder en beskrivelse af krav til sikkerhedsløsning hhv. forventninger til sikkerhedskoncept.

2. Fælles arkitekturrammer

2.1 Vilkår og rammer

Omkring grunddataprogrammet og adressedataprogrammet er der fastlagt en række vilkår for de forskellige projekter og arkitekturen i de løsninger, som udvikles gennem disse.

Disse vilkår er defineret i de aftaler, som er indgået på grunddataniveau hhv. de aftaler der er indgået omkring grunddataprogrammet.

Gennem disse aftaler er indhold og ansvarsplacering ift. de forskellige grunddataregistre fastlagt ligesom det er fastlagt, at grunddata skal distribueres til de forskellige anvendere gennem den fællesoffentlige datafordeler.

Men udover de gennem disse aftaler fastlagte fælles vilkår er der også en hel del andre fælles arkitekturrammer – enten defineret på grunddataprogram niveau eller på adressedata programniveau.

Formålet hermed er bl.a. sikring af:

- Sammenhæng på tværs af de forskellige grunddataregistre.
Omfatter at grunddata udstilles ud fra en fælles begrebsmodel i en sammenhængende arkitektur, baseret på fælles tekniske standarder, sikkerhedsmodeller etc.
- Ensartet udseende ift. anvendere af grunddata.
Dvs. ensartet struktur, navngivning, formater (eksempelvis datoformater) m.m.

2.2 Anvendelse af arkitekturrammer

Opstilling af fælles arkitekturrammer har til formål at styre udviklingen af it-løsninger i den retning, som adressedataprogrammet ønsker.

Der er tale om en "følg eller forklar"-model, dvs. at de fælles arkitekturrammer skal følges med mindre man i det konkrete tilfælde har væsentlige argumenter for at bryde disse.

2.3 Videreudvikling af arkitekturrammer

P.t. er det ikke alle fælles arkitekturrammer, som er fastlagt.

Fælles arkitekturrammer af betydning for adressedataprogrammets målarkitektur er fastlagt i nødvendigt omfang, men ift. de enkelte aftalepartners løsningsarkitektur udestår der en række præciseringer og/eller beslutninger.

Her er der op til den enkelte aftalepartner – i tæt samarbejde med adressedataprogrammet – at sikre en rettidig fastlæggelse af disse fælles arkitekturrammer.

3. Udstilling af grunddata

3.1 Services – Udstilling og anvendelse

Grunddatasystemers læsning af andre grunddata

Når grunddatasystemerne skal læse data i andre grundregistre, f.eks. i forbindelse med validering af opdatering af egne grunddata, sker det gennem Datafordeleren, med mindre der er vægtige forretningsmæssige argumenter for at omgå Datafordeleren. Vurderingen af argumenter og beslutning om at omgå Datafordeler sker på grunddataprogram niveau.

Grunddatasystemers læsning og opdatering af andre grunddata registre

I det omfang der er behov for at læse data i eksterne registre i forbindelse med ajourføring af oplysninger i dette register (via en "Ajourførings-service"), bør ajourførings-serviceen hente data direkte i grunddataregisteret.

Såfremt de grunddata, der skal ajourføres, hentes via Datafordeleren, er der en risiko for, at opdateringen sker på et ikke gældende grundlag.

Sammensatte services

Datafordeleren udstiller services, som sammenstiller data fra flere grunddata registre, f.eks. udstilling af en adresse med tilhørende bygning.

Beslutningen, om hvilke sammensatte service der udstilles, ligger på programniveau ud fra en vurdering af de forretningsmæssige behov.

Specifikation af servicen kan enten ske i et samarbejde mellem de involverede dataejere, foretages af den grunddatamyndighed der er ansvarlig for hovedbegrebet, eller udvikles på programniveau.

Ansaret for specifikationen besluttet samtidigt med beslutningen om etableringen af servicen, på programniveau.

Spatial analyse

Grunddata anvender en del geoobjekter. Spatial analyse anvendes i den forbindelse til etablering af relationer mellem grunddataobjekter på baggrund af deres geografiske placering, f.eks. findes en adresses tilhørsforhold til sogneinddeling på baggrund af adressepunktet.

Spatial analyse implementeres i udstillingsservices på Datafordeleren, som understøtter dette.

3.2 Services – Navngivning og formater

Navngivning af services

Navngivning af såvel udstillings- som ajourførings-services følger de regler, som opstilles af datamodelprojektet.

Problemstillingen omkring services, som sammenstiller data fra forskellige objekter, skal håndteres løbende.

Navngivning for servicestruktur

Navngivning af servicestrukturer følger de retningslinjer som datamodelprojektet leverer.

Fælles dataformater i forhold til services

For data som er omfattet af INSPIRE, efterleves de krav/standarder som er defineret her. Desuden efterleves de krav, som opstilles af datamodelprojektet, om anvendelse af generiske datatyper, f.eks. for tidsangivelse og geografi samt formentlig koder for fælles egenskaber.

Serviceprincipper

I Grunddataprogrammet er der behov for en sammenhængende arkitektur på tværs af de enkelte grunddataregistre og Datafordeler. Derfor skal de enkelte løsninger overholde de 12 grundlæggende serviceprincipper for webservices, der er udviklet i fællesoffentligt regi.

Disse findes beskrevet på: http://arkitekturguiden.digitaliser.dk/serviceprincipper_pr_04.06.2014. En frossen kopi af de opdaterede OIO principper er vedlagt som bilag 12.

3.3 Metadata

Udstilling af metadata

Datamodelprojektets minimumskrav til udstilling af metadata – herunder krav identificeret med udgangspunkt i INSPIRE - skal opfyldes¹. I det omfang grunddataregistret ikke umiddelbart kan leve op til disse krav, kan det vurderes hvorvidt metadata i stedet skal etableres direkte i Datafordeleren.

Metadata udstilles via Datafordelerens metadatakatalog i selvstændige operationer, hvilket gør det muligt at hente metadata uden samtidig at hente forretningsdata.

“Modelregler for grunddata” stiller krav om dokumentation af registrenes udstillingsmodel i form af beskrivelser af alle model-elementer (klasser, attributter, relationer) inkl. bl.a. navn og definition. Beskrivelserne er indlejret i og vedligeholdes sammen med UML-modellen.

Registermyndighederne har ansvar for at specificere services for deres grunddata og på den måde sikre, at relevante metadata leveres i tilknytning til data. Oversigt over data såvel som metadata vil på den måde blive tilgængelige på Datafordelerens metadatakatalog.

Registermyndighederne kan vælge at konstruere services således, at det er muligt, at vælge om objektdefinitioner skal leveres indlejret i data eller i dokumentet/instansen.

Den enkelte grunddatamyndighed kan have et behov for at kunne udstille yderligere metadata, hvilket er tilfældet i GD1 og muligvis også for Adresseprogrammet.

Der kan være et behov for at kunne vedligeholde og udstille et stort og dynamisk metadata-sæt, som skal anvendes i brugergrænseflader i brugervendte systemer og til generering af skriftligt baggrundsmateriale til forståelse af data-rapporter mv.

Det anses **ikke** for formålstjenligt at opbevare disse metadata i Grunddatamodellen, idet deres dynamiske vedligeholdelse vil kræve dels specifikke brugervendte integrationer til den fællesoffentlige datamodel, dels en uhensigtsmæssigt kort opdateringscyklus for denne datamodel.

Derudover kan grunddatasystemet have brug for nogle af de samme metadata i grunddatasystemerne (ifb. ajourføringsservices, brugerflader mv.), hvorfor disse metadata ikke kun bør forefindes i en UML-model på Datafordelerens metadata repository, men også i grunddataregistret.

For at undgå dobbeltvedligehold af disse supplerende metadata, vedligeholder GD1 og GD2 derfor disse metadata i tabeller i egne systemer og kan eventuelt modellere og udstille dem på

¹ Det forudsættes at datamodelprojektet såvel vil beskrive krav til metadata på datasæt-og dataservice niveau og metadata på instansniveau, herunder om instansens (objektets) oprindelse og kvalitet.

linje med andre grunddata samt specificere Datafordeler-services, der udstiller dem på en måde der tilgodeser disse metadatas systembrugere.

3.4 Historik og nøgler

Udstilling af historiske data

Den enkelte registermyndighed afgør ud fra en forretningsmæssig vurdering, hvilke data der udstilles historik for, og hvornår data betragtes som forældede.

Ved udstilling af historik opfyldes kravene til tidsmæssige egenskaber (jf. kapitel 4.2).

Udstilling af registrerede fremtidige data

Den enkelte registermyndighed afgør ud fra en forretningsmæssig vurdering, hvilke data der udstilles med en fremtidig registreret virkningsperiode.

Ved udstilling af fremtidig registreret virkningsperiode opfyldes kravene til tidsmæssige egenskaber (jf. kapitel 4.2).

3.5 Dokumentationskrav

Dokumentation af systemer og systemsammenhænge

Dokumentation af objekter som udstilles i datafordeleren følger datamodelprojektets krav. Øvrig dokumentation, f.eks. protokoller, servicemønstre, endepunkter, systemer og registre er op til den enkelte registermyndighed, dog anbefales det, at man følger de offentlige anbefalinger f.eks. fra Ministerierne Projektcentret (MPK) eller OIOEA.

Forretningsmæssig beskrivelse af services og serviceoperationer

Services og serviceoperationer beskrives ud fra den beskrivelsesramme der leveres af Datamodelprojektet. Som sådan skal beskrivelser af ønskede services referere til modellen.

3.6 Ansvar for services

Ansvar for specifikation af datafordelerens services

Ansvar for specifikation og funktionstest af services udstillet gennem datafordeleren, er placeret hos den enkelte ressortmyndighed.

En del af disse services vil anvende indhold fra mere end ét grundregister. Her vil det være ressortmyndigheden med ansvar for hovedobjektet (jf. begrebsmodellen) som har ansvaret for specifikation og funktionstest af den tilhørende service.

Ansvar for udvikling af datafordelerens services

Ansvar for udvikling af de enkelte services i Datafordeleren skal aftales konkret i det enkelte tilfælde. Det forventes at udviklingen af disse services vil blive foretaget af Datafordeler projektet på baggrund af den specifikation, som ressortmyndigheden har leveret.

Ansvar for udvikling af ajourførings-services

Ansvar for specifikation, udvikling og funktionstest af ajourførings-services ift. de enkelte grunddataregistre er placeret hos den enkelte ressortmyndighed.

4. Grunddata - Generelle egenskaber

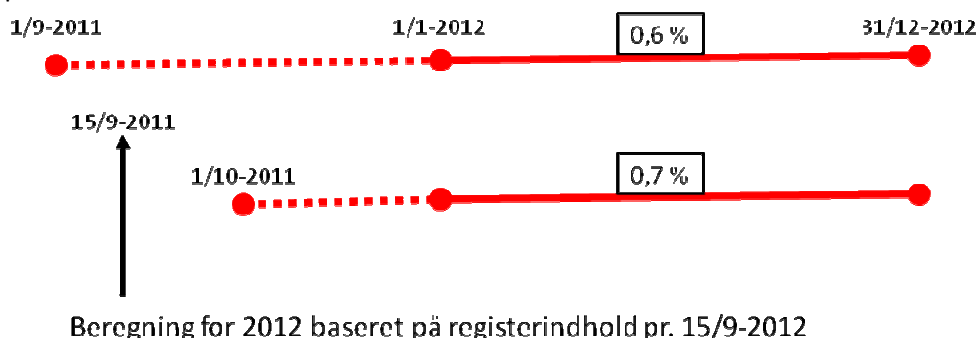
4.1 Tidsmæssige egenskaber - Dobbelthistorik

Dobbelthistorik handler om, at alle forretningsobjekter registreres versioneret, således der over tid altid er styr på et forretningsobjekts aktuelle og historiske informationsindhold. Dette i form af en registrering af en virkningsperiode ("Virkningstid") og en registreringsperiode ("Registreringstid") på den enkelte forekomst af forretningsobjektet.

Registrering af dobbelthistorik er relevant, fordi det sikrer sporbarhed i de registrerede og distribuerede forretningsobjekter. Det offentlige forvaltningsgrundlag skal kunne understøtte, at det til enhver tid er muligt at fremfinde og dokumentere det datamæssige forvaltningsgrundlag (historiske beslutningsgrundlag), der har dannet grundlag for en konkret beslutning/sagsbehandling. Det skal være muligt at fremsøge, hvad der på et givet tidspunkt har været registreret i registret omkring et konkret forretningsobjekt.

I Grunddataprogrammet er der ifb. udstilling af data på den fællesoffentlige Datafordeler behov for en stringent måde at definere registreringstid og virkningstid på. Dette er vigtigt, fordi data skal kunne sammenstilles på tværs af registre og dermed danne grundlag for en bedre og mere effektiv brug af de offentlige grunddata.

Eksemplet nedenfor illustrerer denne anvendelse:



Figur 1. Eksempel: Virkningstid og registreringstid ift. grundskyldsprocent.

I eksemplet registreres 1/9-2011 en grundskyld på 0,6% gældende for hele 2012. Den 15/9-2011 foretager "Aktør A" en beregning for 2012 baseret på denne værdi (0,6%).

1/10-2011 ændres grundskylden til 0,7% ligeledes gældende for 2012. Denne registrering overtrumfer den oprindelige grundskyld på de 0,6%, hvilket betyder, at hvis en aktør efter 1/10-2011 slår op i registret for at få oplysningen, vil aktøren få svaret 0,7%.

Udfordringen er, at "Aktør A" har behov for at kunne dokumentere, at hans beregning er baseret på registerindholdet pr. 15/9-2011 – også efter den 1/10-2011.

Ved at registret forsynes med to forekomster af objektet – begge med virkningstid 2012 men med hvert sit registreringstidspunkt (hhv. 1/9-2011 og 1/10-2011) – er det muligt at leve op til disse krav.

Den konkrete udformning af de tidsmæssige egenskaber ("bitemporale egenskaber") er beskrevet ifb. Grunddataprogrammets modelregler (version 1.1).

5. Hændelser og fejlmelding

5.1 Hændelser

5.1.1 Anvendelse af hændelsesbeskeder

Arkitekturen baseres på kommunikation af indtrufne hændelser i form af hændelsesbeskeder. Hændelsesbeskeder anvendes af grunddatasystemer og andre systemer til at informere hinanden om indtrufne hændelser, som har betydning for et specifikt system - uden at systemet eller sagsbehandleren selv behøver at opsøge informationen rundt omkring i relevante systemer og informationskilder.

Det system, hvori hændelsen er indtruffet, udstiller information om denne hændelse, mens andre systemer så kan abonnere på denne hændelse.

Ejendomsdataprogrammet og Adresseprogrammet har behov for at kunne sende og modtage hændelsesbeskeder internt mellem registrene samt for at kunne modtage hændelsesbeskeder fra hhv. CPR og CVR.

5.1.2 Definition af hændelsesbeskeder

Den enkelte registermyndighed afdækker – i et samarbejde med hændelsesanvendere - de forretningsmæssige behov for hændelser og stiller de nødvendige krav hertil.

Hændelsesanvendere og den registermyndighed der er ansvarlig for generering af hændelsen, afgør sammen, ud fra en forretningsmæssig vurdering, hvilke forretningshændelser der skal udstilles samt hvilke forretningsdata, hvis nogen, en given hændelsesbesked skal indeholde.

Hvis ikke alle relevante data medsendes i hændelsesbeskeder (fx et før- og efterbillede ifb. en opdatering af et objekt), vil der være behov for en udstillingservice, som anvenderen kan kalde for at få adgang til den nødvendige supplerende information.

5.1.3 Generering og udstilling af hændelsesbeskeder

Datafordeleren implementeres således, at den understøtter dannelse af hændelsesbeskeder ud fra data leveret af registrene i GD1 og GD2 samt fra CPR og CVR.

Datafordeleren/Beskedfordeleren understøtter distribution af hændelsesbeskeder til registrene i GD1/GD2 og til dataanvendere. Dette uanset om hændelsesbeskeder er genereret af Datafordeleren selv eller af det enkelte register og videregivet derfra til den fællesoffentlige Datafordeler/Beskedfordeler.

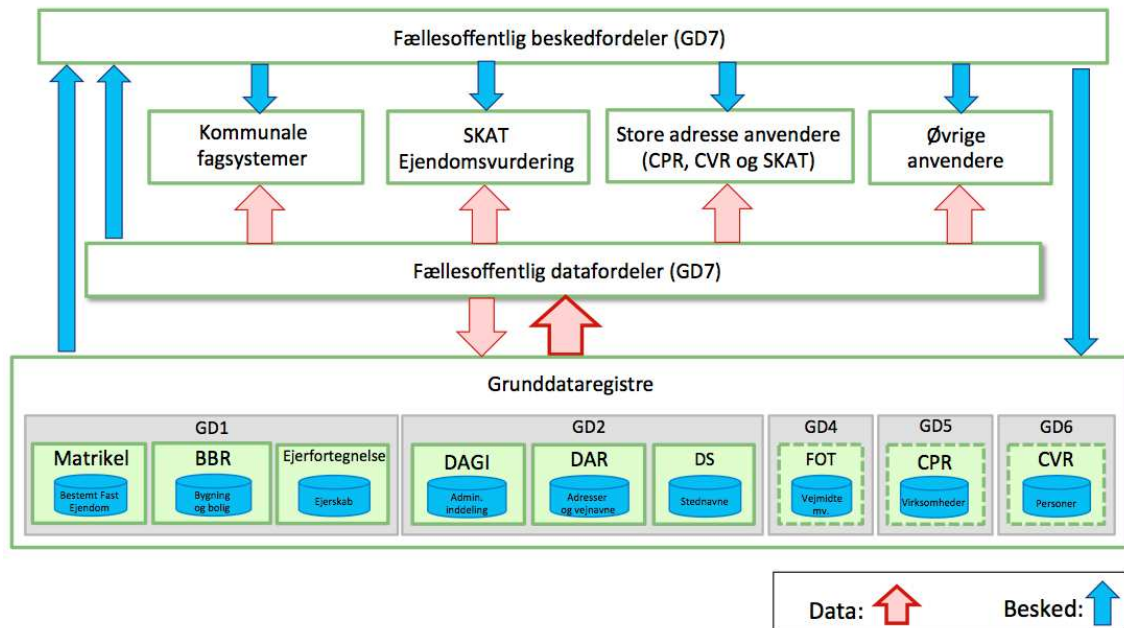
Det er op til den enkelte registermyndighed selv at afklare, hvorvidt hændelsesbeskeder skal genereres af Datafordeleren ud fra data leveret af registret, eller om registret selv vil stå for genereringen af de relevante hændelsesbeskeder.

Ifb. Datafordeleren/Beskedfordeleren kan de enkelte registre og andre anvendere tegne et abonnement på lige præcis de hændelsesbeskeder, som er relevante for dem.

Dette abonnement kan opsættes maskinelt og/eller gennem de dedikeret brugerflade.

Abonnementet kan afgrænses geografisk (fx til en DAGI-inddeling), være på en konkret hændelse, på værdier/værdiskift i attributter (fx et statusskift til "gældende") mv.

Nedenstående figur illustrerer hvordan Datafordeleren/Beskedfordeleren i samarbejde med grunddataregistrene sikrer at princippet om samarbejdende grunddataregistre kan realiseres.



Figur 2. Hændelsesbeskeder og data mellem samarbejdende grunddataregistre.

5.2 Fejlmelding

Behov for fejlmelding

Med gennemførelse af autoritative grunddata øges presset på validiteten af disse grunddata. Anvendere kan ikke længere "blot" rette fejlen i eget register, men er afhængig af at grunddata i en smidig og hurtig proces bliver rettet op.

Der er med andre ord behov for en "fejlmeldingsløsning", som dels kan kommunikere fejlmeldinger til den registeransvarlige, dels kommunikere behandlingen af fejlmeldingen tilbage til anmelder af den pågældende fejl.

Fejlmeldeløsning

P.t. er det ikke afklaret om der skal være en generel fejlmeldeklent i tilknytning til datafordeleren – det er jo der anvenderen oplever fejlen – eller om der skal bygges fejlmeldeklentier i relation til de enkelte grunddataregistre.

Det er vigtigt, at dette bliver afklaret inden løsningsarkitektur omkring de enkelte grunddataregistre fastlægges.

6. Sikkerhed

6.1 Krav til sikkerhed

Grunddataregistre indeholder en række oplysninger, som er forbundet med fortrolighed, og som derfor kun må udleveres til anvendere med rettigheder hertil. Det er derfor vigtigt, at ikke kun grunddataregistrene men også de udstillede services i Datafordeleren er baseret på et tillidsfuldt sikkerhedskoncept, som kan sikre data mod uautoriseret adgang.

Det er et krav, at der omkring udstilling af data via Datafordeleren anvendes samme sikkerhedsniveau, som i de tilhørende grunddataregistre. Det skal ikke være muligt at få uautoriseret adgang til data i Datafordeleren, som man ikke har adgang til i selve grunddataregistret. Sikkerhedsløsningen skal kunne godkendes af Datatilsynet.

Sikkerhedsløsningen skal implementeres, således at denne sikrer en hensigtsmæssig understøttelse af tværgående processer, hvor en bruger arbejder på flere underliggende grunddataregistre samtidig. Situationen vil være uholdbar for den enkelte bruger - fx den kommunale medarbejder - hvis vedkommende skal logge ind individuelt på hvert enkelt grunddataregister hhv. på Datafordeleren, hver gang der skal hentes eller opdateres data – eller hvis brugernes adgang skal administreres i mange forskellige brugerrettighedssystemer.

Dette fordrer en sikkerhedsløsning, som understøtter "Single Sign-on" på tværs af grunddataregistre og Datafordeleren. For de kommunale brugere er der derudover behov for, at sikkerhedsløsningen hænger sammen med de løsninger til brugeradministration og adgangsstyring, der er ved at blive implementeret under den fælleskommunale rammearkitektur i regi af KOMBIT.

6.2 Sikkerhedskoncept

I Grunddataprogrammet er der vedtaget et fælles sikkerhedskoncept, som de enkelte grunddataregistre skal følge. Sikkerhedskonceptet understøtter, at aktører i en og samme arbejdsgang og med ét log-on kan opdatere et eller flere grunddataregistre og samtidig få adgang til grunddata fra Datafordeleren.

Digitaliseringsstyrelsen har i samarbejde med GD1/GD2 og KOMBIT udarbejdet et udkast til fælles sikkerhedsmodel for Grunddataprogrammet. Modellen er baseret på fællesoffentlige anbefalinger og standarder - herunder anvendelse af OIOSAML og identitetsbaserede webservice (IDWS).

Implementeringen af sikkerhedsmodellen gennemføres i to faser:

- Fase 1 baseret på en systembrugermodel
- Fase 2 baseret på en personbrugermodel

Både system- og personbrugermodellen er funderet på en token-baseret adgangsstyring, hvor adgang til en brugerflade eller en web service opnås ved præsentation af et security token (SAML Assertion) udstedt af en betroet tredjepart. Et security token indeholder information om klientens eller brugerens identitet samt tildelte rettigheder i form af roller, og er signeret for at sikre dets autenticitet og integritet.

Security tokens kan udstedes til enten en personbruger eller en systembruger. Forskellen mellem disse er primært, hvor og hvordan brugerstyringen foretages hhv. hvilket system, der har ansvaret for, at brugerne kun får adgang til de funktioner og data, de er berettiget til.

6.3 Brugere og brugerroller

Brugere vedligeholdes i decentrale brugerkataloger hos de autoritative myndigheder, hvor de er ansat, eller hvor adgangen for eksterne brugere naturligt administreres. Dette kan fx være kommunernes egne brugerkataloger.

Brugere tildeles en eller flere brugerroller, som anvendes til at afgøre, hvilke handlinger en bruger må udføre i et grunddatasystem og/eller på Datafordeleren. Brugerrollen fastlægger de rettigheder, som brugeren er tildelt og anvendes til at afgøre om en bruger må udføre en specifik handling på et givet objekt.

Når en klient eller et system i Grunddataprogrammet skal anvende en ajourføringsservice fra et andet register, kræver sikkerhedsmodellen, at der defineres en specifik brugerrolle til sikring af denne adgang.