Direktoratet for samfunnssikkerhet og beredskap

INTERN

DSBs arkitekturprinsipper

Innholdsfortegnelse

Arkitekturprinsipper – oppsummering

DSBs arkitekturprinsipper skal gjelde ved all nyutvikling, anskaffelser eller større endringer knyttet til applikasjonsporteføljen i DSB.

Formålet med arkitekturprinsippene er:

- Sikre at applikasjonsporteføljen blir ensartet og spiller sammen på en optimal måte
- Sikre en effektiv applikasjonsforvaltning og drift
- Sikre at applikasjonene oppleves som hensiktsmessige og lett tilgjengelige
- Sikre at kravene til informasjonssikkerhet blir ivaretatt

Utgangspunktet for DSBs arkitekturprinsipper er prinsippene som er utarbeidet av DIFI. For hvert av de 7 hovedprinsippene er det beskrevet konsekvenser eller hva prinsippet betyr for DSB.

Konsekvensen for applikasjonseiere vil være at all nyutvikling og endringer av applikasjoner skal forholde seg til arkitekturprinsippene. Ved anskaffelser skal arkitekturprinsippene inngå som en del av kravspesifikasjonen. Avvik fra arkitekturprinsippene skal begrunnes og dokumenteres. Applikasjonsforum skal påse at prinsippene blir tilstrekkelig vektlagt i alle saker som applikasjonsforum behandler.

Arkitekturprinsipper – formål og bakgrunn

Formålet med DSBs arkitekturprinsipper er:

- Sikre at applikasjonsporteføljen blir ensartet og spiller sammen på en optimal måte
- Sikre en effektiv applikasjonsforvaltning og drift
- Sikre at applikasjonene oppleves som hensiktsmessige og lett tilgjengelige
- Sikre at kravene til informasjonssikkerhet blir ivaretatt

DSBs arkitekturprinsipper legger de prinsipper som er utarbeidet av DIFI til grunn. DIFI har beskrevet 7 forskjellige prinsipper som er obligatoriske for statlige virksomheter. Disse prinsippene skal alltid legges til grunn og vurderes ved nyutvikling, nyanskaffelser og større applikasjonsmessige endringer.
DIFIs 7 arkitekturprinsipper er knyttet til følgende områder:

- Tjenesteorientering
- Interoperabilitet
- Tilgjengelighet
- Sikkerhet
- Åpenhet
- Fleksibilitet
- Skalerbarhet

En nærmere beskrivelse av DIFIs gjeldende arkitekturprinsipper finnes her:
http://www.difi.no/filearchive/arkitekturprinsipper-2.1.pdf

Prinsippene skal også bidra til at DSB forholder seg til det til enhver tid gjeldende lovverk.

DSB har vurdert det som hensiktsmessig å beskrive mer detaljert hva de 7 forskjellige prinsippene betyr for DSB og hvilke konsekvenser disse prinsippene skal ha.

Tjenesteorientering

Prinsipp	Funksjonalitet og ytelsesnivå skal være hovedhensyn ved utvikling av IT-løsninger. IT-tjenester som er nødvendig for å understøtte hele eller deler av en eller flere arbeidsprosesser skal identifiseres.
DIFIs forklaring	Prinsippet skal understøtte strategisk, effektiv og kostnadseffektiv bruk av IT ved å ta hensyn til hvilke tjenester (i forståelsen funksjonalitet) som leveres av en komponent, fremfor hvordan komponenten er sammensatt. Dette bidrar til å bryte opp siloer, både innad i egen virksomhet og på tvers av sektorer, som igjen legger til rette for gjenbruk. Komponenter kan være nasjonale felleskomponenter, sektorvise felleskomponenter eller virksomhetsspesifikke komponenter. Ved å legge til rette for gjenbruk av tjenester og komponenter i virksomheter og på tvers av offentlig sektor, der det er hensiktsmessig, bidrar prinsippet om tjenesteorientering til raskere og mer kostnadseffektiv utvikling av elektroniske tjenester.
Konsekvenser for DSB – underprinsipper	Ved anskaffelse eller utvikling av nye løsninger, samt større endringer av eksisterende løsninger skal følgende beskrives: • Hvilke deler av løsningens funksjonalitet som kan være av interesse for andre deler av virksomheten og hvordan dette kan brukes av andre • Hvilke deler av løsningens funksjonalitet som kan være av interesse for andre statlige virksomheter og hvordan dette kan brukes av disse virksomhetene • Hvorvidt det finnes eksisterende tjenester i egen virksomhet som kan levere ønsket funksjonalitet, helt eller delvis • Hvorvidt det finnes eksisterende tjenester utenfor egen virksomhet som kan levere ønsket funksjonalitet, helt eller delvis

Interoperabilitet

Prinsipp	Virksomheten og dens IT-løsninger må ved behov kunne samhandle med andre relevante virksomheter og deres IT-løsninger på et hensiktsmessig nivå.
DIFIs forklaring	Prinsippet skal legge til rette for effektiv informasjonsflyt og sikre at den samlede IT-utvikling i staten støtter godt opp under arbeidsprosesser og regelverk, både innen den enkelte virksomhet og på tvers av offentlige virksomheter. Prinsippet skiller mellom tre ulike typer interoperabilitet: • **Organisatorisk interoperabilitet** Innebærer samordning av arbeidsprosesser, avtaleverk og endringer av organisatoriske forhold nødvendig for samhandling • **Semantisk interoperabilitet** Innebærer å avklare meningsinnholdet for informasjonselementene som utveksles • **Teknisk interoperabilitet** Innebærer å bruke tekniske standarder som legger til rette for veldefinerte grensesnitt, overføringsprotokoller og formater Det er en forutsetning for interoperabilitet at det ikke foreligger noen juridiske begrensninger for samhandlingen. Juridiske vurderinger er også sentrale som en del av både organisatorisk og semantisk interoperabilitet.
Konsekvenser for DSB – underprinsipper	Det skal beskrives hvilke deler av virksomheten som berøres av løsningen, både direkte og indirekte. Avhengigheter (tekniske og organisatoriske) skal spesifiseres. Det skal også beskrives i hvilken grad løsningen skal samhandle med andre relevante virksomheter. Ved utveksling av informasjon eller publisering av informasjon skal Referansekatalog for IT-standarder i offentlig sektor legges til grunn. Der denne ikke gir anvisning på aktuelle standarder, skal åpne standarder benyttes. Løsningen skal gjøre gjenbruk av dataelementer som allerede finnes for å redusere behovet for dobbeltlagring av informasjon (innordne seg ifht DSBs fremtidige regime for Master Data Management).

Tilgjengelighet

Prinsipp	Elektroniske tjenester skal være tilgjengelig når brukerne trenger dem, lette å finne frem til og brukervennlig og universelt utformet.
DIFIs forklaring	Prinsippet skal legge til rette for gode og brukerrettede elektroniske tjenester ved å sørge for at de er tilgjengelig for alle som har behov for dem, til den tid de har bruk for dem, og på en måte som gjør det mulig for dem å ta tjenestene i bruk. Tjenestene skal kunne benyttes av alle relevante brukergrupper, uavhengig av alder, kjønn, funksjonsevne og kulturell / etnisk bakgrunn. Tjenestene skal være utformet slik at ingen brukergrupper blir diskriminert.
Konsekvenser for DSB – underprinsipper	Punktene som er beskrevet nedenfor dekker både elektroniske tjenester til brukere utenfor DSB og løsninger som brukes internt i virksomheten. **Brukertilpasning** De elektroniske tjenestene skal være enkle å finne frem til og skal ikke forutsette at brukerne kjenner til hvordan forvaltningen er organisert. I tillegg til at informasjonen tilgjengliggjøres på norsk, skal den også tilgjengliggjøres på andre språk dersom det er rimelig å anta at løsningen vil brukes av fremmedspråklige. **Åpningstid** Tjenestene skal være tilrettelagt for at den skal være tilgjengelige 24/7. **Teknologiuavhengig for eksterne brukere** Så langt det er mulig bør elektroniske tjenester til eksterne være teknologi- og plattformuavhengig, slik at det ikke stilles krav om bruk av bestemte løsninger eller produkter for å benytte tjenestene. **Kanalvalg** Tjenesten skal være tilgjengelig på de kanaler (PC, mobiltelefon, brett, mv.) som er relevante og egnet, men likevel være forutsigbar og gjenkjennelig. Med relevant menes relevant sett fra brukernes ståsted. **Tilgangskontroll** Hovedprinsippet skal være at løsningen skal være tilrettelagt for DSBs Single SignOn regime. For løsninger som av ulike årsaker krever større tilpasninger for at prinsippet skal kunne innfris, skal det gjøres en kost/nytte og risikovurdering før det besluttes om prinsippet skal implementeres i løsningen.. Implementering av prinsippet innebærer at DSBs til enhver tid gjeldende tilgang- og autentiseringsverktøy skal håndtere tilgangskontrollen og det skal ikke være nødvendig å foreta spesifikk pålogging til løsningen etter at en har logget seg på og blitt identifisert i DSBs interne nett. **Brukergrensesnitt** Brukergrensesnittet skal være intuitivt og tilpasset de arbeidsoppgaver som skal utføres. **Dokumentasjon**

	Brukerdokumentasjon skal være tilgjengelig elektronisk og være søkbar. Ved behov for funksjonell støtte skal en enkelt søke seg frem til relevant område i dokumentasjonen. **Teknologi** Løsningen skal være teknologi og plattformuavhengig og skal kunne fungere optimalt på den til enhver tid gjeldende teknologiske plattform som DSB har valgt/installert. **Eksterne avhengigheter** Løsningen skal være designet på en slik måte at den i stor grad eller delvis skal kunne brukes selv om eksterne avhengigheter blir utilgjengelige **Tilgang til nettverk og server** Løsningen bør være tilrettelagt for at enkelte arbeidsoppgaver skal kunne utføres selv om tilgang til nettverk eller sentral server ikke er tilgjengelig. **Informasjonstilgang** Løsningen skal legge til rette for enkel tilgang til all relevant informasjon. Det skal ikke være nødvendig at brukerne skal ha kjennskap til hvor informasjonen er lagret og hvilke system som administrerer informasjonselementene.

Sikkerhet

Prinsipp	IT-løsningen i seg selv og informasjonen som behandles i denne, skal med utgangspunkt i formelle og risikobaserte krav beskyttes mot brudd på konfidensialitet, integritet og tilgjengelighet.
DIFIs forklaring	Sikkerhetsprinsippet skal sikre at offentlige IT-løsninger blir etablert og driftet på en sikkerhetsmessig god måte, samtidig som informasjon og tjenester er elektronisk tilgjengelig for de som har behov for og/eller rettigheter til disse. Prinsippet vil også bidra til å styrke offentlige virksomheters kompetanse, organisering, kultur og regelverksetterlevelsesevne rundt informasjonssikkerhet. Sikkerhetsprinsippet er en viktig forutsetning for å opprettholde tilliten til offentlig sektor. Prinsippet kan blant annet utledes av eForvaltningsforskriften, personopplysningsloven, sikkerhetsloven og regler om taushetsplikt. Enhver elektronisk tjeneste som etableres skal defineres til et gitt sikkerhetsnivå (klassifisering) basert på en risikoanalyse. Tjenesten skal konstrueres slik at sikkerhetsnivået kan endres ved behov. Sikkerhetsnivået må dokumenteres, slik at det blir helt klart for den som tar løsningen i bruk hvilke krav som er oppfylt. Krav til konfidensialitet skal oppfylles. Informasjonen skal beskyttes tilfredsstillende mot innsyn fra uvedkommende. Integritet skal være ivaretatt. Informasjon skal være tilstrekkelig sikret mot utilsiktede eller urettmessige endringer. Som regel må det være mulig å spore hvem som har foretatt endringer og når endringene ble gjort. Informasjonen skal være tilgjengelig i de tidsperioder som er besluttet og innenfor de rammer som er satt for hvem som skal ha tilgang til informasjonen. Tilgangsstyringen må finne en balanse mellom de tjenestlige behov og behovet for konfidensialitet. Sikkerhetsprinsippet kan begrense andre prinsipper, dersom dette er avgjørende fortilliten til offentlig sektor.
Konsekvenser for DSB – underprinsipper	Prinsippet medfører følgende konsekvenser for DSB.: **Tilgangskontroll** Hovedprinsippet skal være at løsningen skal være tilrettelagt for DSBs Single SignOn regime. For løsninger som av ulike årsaker krever større tilpasninger for at prinsippet skal kunne innfris, skal det gjøres en kost/nytte og risikovurdering før det besluttes om prinsippet skal implementeres i løsningen. Implementering av prinsippet innebærer at DSBs til enhver tid gjeldende tilgang- og autentiseringsverktøy skal håndtere tilgangskontrollen og det skal ikke være nødvendig å foreta spesifikk pålogging til løsningen etter at en har logget seg på og blitt identifisert i DSBs interne nett. Implementering av prinsippet innebærer også at det skal være individuell tilgangskontroll og ikke være mulig å operere med felles brukere og/eller passord. **Sikkerhetsmekanismer i løsningen** Anerkjente standarder/mekanismer skal være lagt til grunn for å håndtere kravene til informasjonssikkerhet innad i løsningen.

	Ikke benektning Alle endringer av dataelement (endringer, slettinger og nyregistrering) skal kunne spores til unike brukere. **Ingen dobbellagring av informasjon** Alle informasjonselement skal i prinsippet kun lagres ett sted. Dette for å sikre integritet. **Overvåkning** Løsningen skal være tilrettelagt for å kunne overvåkes i forhold til både tilgjengelighet og integritet. **Rettigheter** Bruk av løsningen skal ikke kreve utvidede rettigheter. Dette innebærer blant annet at en ressurs som er definert som administrator i løsningen ikke skal behøve utvidede systemadministrasjons rettigheter for å kunne fylle rollen som administrator i løsningen.

Åpenhet

Prinsipp	IT-løsningers virkemåte og datagrunnlag skal kunne gjøres rede for.
DIFIs forklaring	Prinsippet skal bidra til å understøtte rettssikkerheten ved at det skal være kjent hvilke premisser som ligger til grunn for avgjørelser. Dette er særlig relevant for IT-løsninger som fungerer som beslutnings- eller beslutningsstøttesystemer og som har betydning for den enkeltes rettigheter eller plikter.
Konsekvenser for DSB – underprinsipper	For DSB så vektlegges det i tillegg til ovenstående at prinsippet skal understøtte virksomhetens behov for å se sammenhengen mellom de ulike applikasjoner og dataelementer, samt hvordan dataelementer fermstilles og utveksles. **Datamodell** Datamodellen skal være beskrevet på både et overordnet og detaljert nivå og det skal være mulig for uinnvidde å forstå sammenhengene i datamodellen. **Programmeringsspråk** De utviklingsverktøy/programmeringsspråk som benyttes skal være anerkjente og utprøvde. **Dokumentasjon** Det skal foreligge overordnet og detaljert designdokumentasjon som viser innholdet i alle løsningens komponenter, hvordan disse komponentene spiller sammen, samt hvilke avhengigheter det er til eksterne komponenter (komponenter utenfor løsningen).

Fleksibilitet

Prinsipp	IT-løsninger skal være utformet slik at de ikke fremstår som begrensende for endringer i arbeidsprosesser, innhold, organisering, eierskap og infrastruktur.
DIFIs forklaring	Prinsippet skal bidra til kostnadseffektivitet ved at IT-løsningene kan tilpasses endrede rammevilkår. Virksomhetens behov og oppgaveløsing skal være hovedhensyn når nye IT-løsninger etableres. Prinsippet skal forstås med det som bakgrunn og handler om å utvikle IT-løsninger slik at de ikke blir ubrukelige eller forutsetter store omleggingar dersom arbeidsprosesser, innhold, organisering, eierskap eller infrastruktur endrer seg. Dette legger til rette for gjenbruk innad i den enkelte virksomhet og på tvers av offentlig sektor.
Konsekvenser for DSB – underprinsipper	Følgende konsekvenser og/eller underprinsipper gjelder for DSB: **Komponentbasert** Løsningen skal være modularisert slik at det ved endringer kun gjøres tilpasninger i den delen av løsningen som er berørt. **Uavhengig av organisasjonsstruktur** Løsningen skal ikke være avhengig av en spesifikk organisasjonsstruktur. Det skal være enkelt å tilpasse løsningen til større organisasjonsmessige endringer og dette skal ikke kreve design eller programendringer. Det skal være mulig å operere med forskjellige juridiske virksomheter i samme instans av løsning. **Standardisert dataaksess** Løsningen skal baseres på verktøy/metoder som er plattformuavhengige ifht aksessering av data og den skal være tilrettelagt for den databaseplattform som til enhver tid er valgt av DSB. Dette innebærer blant annet at standard SQL skal være lagt til grunn ved design og utvikling av løsningen. Dette gjelder spesielt for egenutviklede løsninger og løsninger som skal driftes av DSB selv. **Virtualisering** Løsningen skal være tilrettelagt for å kunne kjøres i et virtuelt server-miljø. **Dokumentasjon** Drifts- og systemdokumentasjon skal ha en kvalitet som sikrer at det er mulig med alternative drifts- og forvaltningsmodeller, uavhengig av om det driftes/forvaltes internt eller eksternt. **Utrulling av løsning** Applikasjonen skal kunne rulles ut ved bruk av utrullingsverktøy som f.eks SCCM **Kanaler** Løsningen skal være tilrettelagt for å kunne nås gjennom flere kanaler (som f.eks mobiltelefon, nettbrett, etc).

Skalerbarhet

Prinsipp	IT-løsninger skal kunne skaleres ved endringer i bruken.
DIFIs forklaring	Prinsippet skal bidra til bevisstgjøring av viktigheten av at IT-løsninger fortsatt kan benyttes, selv om graden av utnyttelse endrer seg. Endring kan være knyttet til antall brukere, volum, responstider, eller IT-løsningens livsløp
Konsekvenser for DSB – underprinsipper	For DSB vil det være viktig å sikre at løsningens konstruksjon ikke er til hinder for opp- og nedskaleringen i forhold til bruk av løsningen. **Virtualisering** Løsningen skal være tilrettelagt for å kunne kjøres i et virtuelt servermiljø. **Dynamisk backup, failover og lastballansering.** Løsningen skal være designet slik at DSB til enhver skal kunne ha en oppdatert sikkerhetskopi av løsningen. Spesifikt skal en kunne legge opp til lastballansering, failover og at løsningen skal kunne skaleres over flere noder. **Differensiert kapasitet.** Kapasiteten skal enkelt kunne økes i perioder med spesielt stor bruk og deretter tas ned igjen. **Datamodell** Datamodellen skal være designet slik at behovet for tilhørende infrastruktur utvikler seg linjert i forhold til hvordan løsningen utnyttes og hvordan datamengden endrer seg. **Avtalte tjenesteleveranser** Det må legges til rette for at tjenesten som avtales må kunne skaleres opp eller ned basert på det til enhver tid gjeldende behov. Avtalene som inngås skal ta hensyn til opp- og nedskalering av hvordan løsningen brukes. Opp- eller nedskalering skal også reflekteres i prismodellen.

Direktoratet for
samfunnssikkerhet og beredskap
Postboks 2014
3115 Tønsberg

Tlf. 33 41 25 00 postmottak@dsb.no
Faks 33 31 06 60 www.dsb.no