Ministeriet for Ligestilling og Kirke

Arkitekturprincipper for Kirkenettet
- Bilag 2 til It-Strategi 2013-2015

Arkitekturprincipperne består af 27 principper, som det er obligatorisk at overveje ved nyanskaffelser og større ændringer af eksisterende fagsystemer.

Arkitekturprincipperne skal sikre, at ændringer og nyanskaffelser sker i henhold til en defineret målarkitektur, som hele tiden justeres i takt med, at nye teknologiske muligheder opstår.

Overholdelse af principperne skal sikre, at

- systemanskaffelser og/ eller større ændringer til eksisterende systemer overvejes i forhold til de behov, der er, herunder at muligheden for at ændre på arbejdsgange er blevet overvejet. I den forbindelse skal det overvejes, om en standardløsning kan anvendes frem for en dyrere specialudvikling. [1-8]
- systemerne i Kirkenettet kan kommunikere indbyrdes og i samspil med systemer i andre driftsmiljøer, herunder at systemerne i Kirkenettet lever op til målsætningerne i Digitaliseringsstrategien. [9-14]
- systemerne er sikre, hvilket betyder, at persondataloven kan overholdes, ligesom hensyn vedrørende tilgængelighed, autenticitet og fortrolighed tilgodeses. [15-20]
- systemernes performance er tilstrækkelig, ligesom den nødvendige driftstid vurderes. [21-22]
- systemerne er betjeningsvenlige og så vidt muligt med et layout og en betjeningslogik, som svarer til den, som ses i andre systemer i Kirkenettet. [23-27]

Vurderingen af principperne for et givent projekt dokumenteres i forhold til en checkliste, hvor alle arkitekturkravene gennemgås.

Den udfyldte checkliste indgår i beslutningsgrundlaget for projektets gennemførelse.

De 27 principper:

Ministeriet for Ligestilling og Kirke

1.1 Behovsvurdering

1.	OPTIMERING ARBEJDSGANGE VED DIGITALISERING
Definition	Genstanden for et it-projekt, eksempelvis en arbejdsgang eller en struktur, skal vurderes med henblik på forenkling, før it-understøttelse udvikles.
Begrundelse	Der er brug for et billede af såvel den forretningsmæssige som den it-mæssige målarkitektur. Dermed mindskes risikoen for at "asfaltere den slagne vej", hvor en ny vej er bedre. Enkle arbejdsgange eller strukturer er som hovedregel billigere at it-understøtte end komplicerede. Når først it-understøttelsen er på plads, er det typisk dyrere at ændre arbejdsgange eller strukturer.
Konsekvens	Før der anskaffes nye systemer, skal det undersøges, om det er relevant og muligt at omlægge arbejdsgange eller at simplificere strukturer.

2.	FULD IT-UNDERSTØTTELSE ER IKKE EN UBETINGET MÅLSÆTNING
Definition	Fuld it-understøttelse kan have væsentligt større total-omkostninger og medføre flere afledte problemstillinger end en mindre komplet understøttelse.
Begrundelse	At få indarbejdet alle specialtilfælde, eksempelvis undtagelser i den folkekirkelige struktur, er dyrere og modarbejder princippet om at udnytte standardsystemer bedre.
Konsekvens	Totalomkostningen ved at it-understøtte 95 % - 98 % af opgaven i stedet for at gøre det 100 % skal estimeres. En it-løsning, der ikke dækker fuldt ud, kræver løbende en manuel indsats. Omkostningen til denne og risikoen for fejl i behandlingen skal afdækkes for at skaffe et fuldt overblik over økonomien for folkekirken, ministeriet og for samfundet.

3.	SYSTEMANSKAFFELSER VURDERES I FORHOLD TIL HELHEDEN
Definition	Systemanskaffelser og forbedringer vurderes i forhold til et samlet service-, applikations- og integrationslandkort.
Begrundelse	Folkekirkens og ministeriets opgaver skal i stigende grad kunne løses sammenhængende og fleksibelt.
Konsekvens	Enhver service og applikation skal leve op til krav om udveksling af data og/eller indgå i en sammenhængende brugergrænseflade. Service-, applikations- og integrationslandkortene skal opdateres af projekter, der tilføjer eller fjerner systemer, services eller applikationer.

4.	LEVETID OG FORANDRINGSBEHOV
Definition	Hver service og applikation karakteriseres med levetid og forandringsbehov.
Begrundelse	Kravene til en service og applikation vil afhænge af, hvor lang levetid den har, og hvilke løbende forandringsbehov den forventes at have.
Konsekvens	Vurdering af levetid og forandringsbehov skal indgå i opstillingen af krav til applikationen. Lang levetid eller højt forandringsbehov medfører højere krav til overholdelse af it-arkitekturprincipperne. Ved enkle løsninger med kort forventet levetid kan arkitekturprincipperne lettere fraviges. Hvis principperne er blevet fraveget, og levetiden viser sig at være længere end forventet, udestår der en tilpasningsopgave.

5.	STANDARDLØSNINGER FREM FOR EGENUDVIKLING
Definition	Indkøb standardløsninger, før der udvikles egne løsninger.
Begrundelse	Man kan opnå større fleksibilitet ved at anvende standardløsninger, hvor egenudviklede løsninger ofte vil rette sig mod en meget konkret opgave og derfor ikke kan genbruges.
Konsekvens	Ved enhver analyse af behov skal det for hele opgaven og for delopgaver vurderes, om der allerede findes løsninger i Kirkenettet, og/- eller om der findes standardløsninger.

6.	UDNYT STANDARDSYSTEMERNE I STEDET FOR AT KØBE NYT
Definition	Standardsystemerne skal udnyttes bedre og mere effektivt.
Begrundelse	En række standardsystemer udnyttes kun delvist. Uudnyttede funktioner kan eventuelt erstatte nyanskaffelser.
Konsekvens	Før der anskaffes nye systemer, skal det undersøges, om eksisterende systemer kan anvendes. Eksisterende systemer skal periodisk underkastes en undersøgelse af, om de kan anvendes bedre. For at en god udnyttelse kan sikres, skal følgende overholdes: - Uddannelse af brugere / superbrugere af systemerne skal sætte disse i stand til at anvende systemerne mere effektivt, mere innovativt og til flere formål. - Periodisk og systematisk opsamling af forbedringsønsker og oplevede problemer skal danne grundlag for f. eks. uddannelse og tilpasninger med henblik på mere effektiv systemudnyttelse.

7	GENBRUG
Definition	Genbrug løsninger, før der indkøbes nye løsninger.
Begrundelse	Eksisterende løsninger har ofte funktionalitet, som ikke udnyttes, og den skal udnyttes, før der anskaffes nye løsninger.
Konsekvens	Ved enhver analyse af behov skal det for hele opgaven og for delopgaver vurderes, om der allerede findes løsninger i Kirkenettet, og/- eller om der findes standardløsninger.

8	EN SYSTEMEJER ER ANSVARLIG FOR DET FÆRDIGE SYSTEM
Definition	Systemer skal forvaltes efter leveranceforløbet for at sikre gevinst-realisering og fortsat opgaveunderstøttelse, det er systemejerens ansvar.
Begrundelse	It-projekter skaber sjældent værdi i sig selv, men kræver opfølgning og fokus på den organisatoriske implementering, før formålet med projektet er opfyldt, og gevinsterne er realiseret.
Konsekvens	Systemejeren skal udpeges som en del af projektforløbet.

9	BRUG FÆLLESOFFENTLIGE KOMPONENTER
Definition	Løsninger, der er rettet til borgere, virksomheder og andre myndigheder, anvender fællesoffentlige komponenter.
Begrundelse	Der er etableret en række fællesoffentlige komponenter, som kan bruges i Kirkenettet.
Konsekvens	I Kirkenettet skal anvendes fælles komponenter som NemID, NemLog-in, eBoks m.fl.

1.2 Kommunikation og interaktion

10	KOMMUNIKATION MELLEM VIGTIGE SERVICES BASERES PÅ KIRKENETTET
Definition	Kommunikationen mellem services, applikationer og klienter skal baseres på Kirkenettet, som er folkekirkens og ministeriets sikrede netværk.
Begrundelse	Kommunikationen skal overholde høje krav til sikkerhed, hvilket ligger til grund for opbygningen og den fortsatte udvikling af Kirkenettet.
Konsekvens	Folkekirken og ministeriets systemer kommunikerer via Kirkenettet. Da størstedelen af kommunikationen samles i dette område, vil der blive - øget behov for udveksling af information (her skal der anvendes en vifte af teknologier) - øget behov for tidstro udveksling af information; webservices frem for eller i samspil med batch (natlige ajourføringer). Der vil blive større krav til pålideligheden og dermed mere overvågning af processerne. Det betyder krav om at skabe et samlet overblik og senere et ansvar for udvekslingsopgaver.

11	SIKKER KOMMUNIKATION TIL SYSTEMER UDEN FOR KIRKENETTET
Definition	Systemer, som drives uden for Kirkenettet og anvendes af brugere i Kirkenettet (CPR/Den Elektroniske Kirkebog, FLØS (Folkekirkens LønService), Navision, KAS og GIAS m. fl.), skal forbindes med Kirkenettet med tilstrækkelig sikkerhed og kapacitet.
Begrundelse	Kommunikationen skal overholde høje krav til sikkerhed, og disse krav skal også sikres, hvor systemet drives af tredjepart, og hvor der etableres forbindelse fra Kirkenettet til systemet f. eks. over internettet.
Konsekvens	Afhængigt af teknologiske krav, anvendelse og krav til sikkerhed kan der etableres forskellige typer af forbindelser - en sikret tunnel mellem Kirkenet og et eksternt driftscenter - en direkte opkobling fra de enkelte klienter til systemet. Der skal i hvert enkelt tilfælde ske en grundig vurdering af behov og muligheder, før der vælges en løsning.

12	EKSTERNT SYSTEM TIL SYSTEM-KOMMUNIKATION (B2B) BASERES PÅ SOAP OG/- ELLER REST WEBSERVICES
Definition	System til system-kommunikation med eksterne parter baseres på SOAP- og/ eller REST-webservices efter anbefalinger fra Digitaliseringsstyrelsen.
Begrundelse	Ved at stille services og data til rådighed på en åben fællesoffentlig platform skal der i Kirkenettet kun vedligeholdes én type snitflader og én kommunikation med andre. Desuden skal krav om anvendelse af åbne standarder efterleves (B103). Ved system til system- kommunikation med særlige behov (f. eks. store datamængder) skal der tages stilling til, om der kan anvendes andre løsninger, hvis SOAP-og/ eller REST-webservices ikke kan klare opgaven tilfredsstillende.
Konsekvens	Dette krav vedrører den kommunikation, der sker på systemniveau mellem systemer. Der stilles krav til eksterne samarbejdsparter om at efterleve disse standarder, herunder anvendelsen af XML, som er en del af SOAP- og REST-webservices-anbefalingerne. Valget mellem SOAP og REST skal foretages via afvejning af projektets nonfunktionelle krav, herunder sikkerhed. For kommunikation med særlige behov, f. eks. overførsel af data til ledelsesinformation, kan der blive brug for at anvende andre standardiserede løsninger. Såfremt kommunikationen indeholder personfølsomme oplysninger, skal den foregå enten via en sikret tunnel, via direkte netværk eller ved kryptering af beskeden gennem anvendelse af et certifikat.

13	DATA SKAL LÆSES FRA OG OPDATERES I MASTERDATA-KILDEN.
Definition	I et miljø med mange datakilder skal det sikres, at vedligeholdelse af data er konsistent via veldefineret adgang og ajourføring af masterdata.
Begrundelse	Der er brug for at sikre konsistente data, og for at disse er aktuelle. Det kræver, at disse data opdateres i og læses fra samme kilde.
Konsekvens	Data om brugere og installationssteder vedligeholdes autoritativt i KIS. For at være sikker på, at KIS afspejler de seneste data, skal data, der ændres andre steder, opdateres rettidigt i KIS. Kopier af data anvendes kun til læseformål. I det omfang kopidata er nødvendige for f. eks. performance, skal disse opdateres fra masterdata-kilden så hyppigt, at data efterlever de forretningsmæssige krav om korrekthed.

14	VELDEFINEREDE OPLYSNINGER I DATAUDVEKSLINGER
Definition	Betydningen af oplysninger i dataudvekslinger skal være veldefinerede.
Begrundelse	Udveksling af data mellem systemer kræver, at data kan genbruges direkte eller konverteres automatisk, hvilket i begge tilfælde kræver, at data er entydigt defineret på tværs af systemerne.
Konsekvens	En klar og konsekvent organisering af - ejerskab til information og dens repræsentation i data - definition af informationers betydning og datasyntaks informationers klassifikation (taksonomi og begrebsmodel) - datas struktur og relationer (datamodel) - datas placering i tilgængelige metadataløsninger, som skal dokumenteres for nye systemer og ved integrationer.

1.3 Sikkerhed

15	BESKYTTELSE GENNEM VELDEFINEREDE SIKKERHEDSZONER
Definition	Kirkenettets services og applikationer beskyttes mod fjendtlig indtrængning gennem et antal veldefinerede sikkerhedszoner.
Begrundelse	Kirkenettets services og applikationer stiller meget forskellige krav til sikkerheden – og meget høje krav på nogle områder. Desuden er den fysiske afgrænsning til Kirkenettet ikke tilstrækkelig til at håndtere behovene – flere applikationer tilgås over internettet, ligesom der skal være adgang til Kirkenettet "udefra". For at håndtere sikkerhed og fleksibilitet med et overkommeligt ressourceforbrug deles netværket op i et antal sikkerhedszoner.
Konsekvens	Alle systemer skal overholde reglerne for den sikkerhedszone, det er placeret i.

16	HØJ SIKKERHED I GENNEM KRYPTERING, HVOR DET ER MULIGT
	Der skal være høj sikkerhed i kommunikationen fra arbejdspladserne til systemerne, hvilket skal opnås ved kryptering.
	Sikkerhedskravene til systemer som fx Personregistrering er meget høje og kræver stor sikkerhed for adgange til systemerne og sikrer samtidig mod andres uretmæssige adgang dertil.
	Kommunikationen mellem arbejdspladser og systemet skal være krypteret. Systemer skal anvende og forcere tilgængelige krypteringsmetoder (fx HSTS), hvor det er muligt.

17	SPORBARHEDSLOGNING AF BRUGEN AF SYSTEMER
Definition	For alle systemer skal der udføres en sporbarhedslogning af grupperne personregisterførere, borgere og administratorer.
Begrundelse	Uanset hvor sikkert et system er, vil der være risiko for uretmæssig anvendelse. Det er derfor vigtigt, at alle hændelser logges, og at loggen overvåges og analyseres, så misbrug opdages og efterforskes.
Konsekvens	For ethvert system skal der ske en vurdering af niveauet for logning, analyse og kontrol i forhold til en vurdering af risiko for og konsekvens af sikkerhedsbrud. For kritiske systemer som CPR og Den Elektroniske Kirkebog skal der gennemføres systematisk analyse og kontrol af loggen. Ansvaret for logning samt overvågning og analyse af loggen skal placeres, og der skal udarbejdes et regelsæt, så det sikres, at overvågningen gennemføres. Der skal være funktionsadskillelse mellem anvendelsessiden af et system og log-arbejdet.

18	ACTIVE DIRECTORY ER KERNEN I STYRING AF RETTIGHEDER
Definition	Microsoft Active Directory (AD) håndterer data om brugere og adgangskontrol, og andre systemer skal anvende data og eventuelt adgangskontrol.
Begrundelse	Med de mange tusinde brugere af Kirkenettets systemer vil det give et for stort ressourceforbrug at skulle administrere brugerne i hvert enkelt system. Det er desuden et sikkerhedsmæssigt krav, at brugere ændres og slettes, når deres adkomst til Kirkenettets systemer ændres (stillingsskift, fratrædelse). Desuden skal brugernes log-in til systemerne begrænses af hensyn til brugervenligheden.
Konsekvens	Kommende nye applikationer indkøbes med krav om brug af AD som minimumsbrug af brugerdata fra AD.

19	MEDARBEJDERCERTIFIKATER TIL SIKRING AF BRUGERNES IDENTITET
Definition	Til autenticitetssikring i log-in til Kirkenettet anvendes snarest muligt NemId.
Begrundelse	Flere og flere medarbejdere skal tilgå eksterne systemer, hvor log-in med NemId er krævet. Ved at bruge NemId til log-in generelt vil brugerne ikke skulle håndtere flere forskellige log-in-situationer.
Konsekvens	Der skal etableres en effektiv udrulning og administration af NemId-medarbejdercertifikater som en del af brugeradministrationen. Brugerne skal uddannes til at håndtere medarbejdercertifikaterne. Identiteten af brugeren sikres under udleveringen af medarbejder-certifikater. Autentificeringen af brugeren over for systemet sker via medarbejder-certifikater. Autorisationen af brugeren sker i forhold til hans/hendes stilling.

20	FOKUS PÅ SIKKERHED VED ÆNDRINGER
Definition	Ved hver ændring af en eksisterende service eller applikation og hver nyanskaffelse skal der være særligt fokus på sikkerheden.
Begrundelse	Særligt ved ændringer i systemer og ved nyanskaffelser opstår der erfaringsmæssigt sikkerhedsmæssige risici, som det kræver opmærksomhed at undgå.
Konsekvens	Der skal ved enhver ændring og nyanskaffelse ske en sikkerhedsmæssig vurdering (risikovurdering) og planlægning af sikkerhedstiltag.

1.4 Drift og performance

21	MONITORÉR OG ESTIMÉR BELASTNING
Definition	Folkekirkens It monitorerer og estimerer belastningen af Kirkenettets services og applikationer.
Begrundelse	For at undgå overbelastning og dermed manglende adgang til applikationer skal belastningen løbende overvåges, og det skal desuden løbende estimeres, hvordan belastningen kan forventes at udvikle sig, særligt i forbindelse med nyanskaffelser og andre ændrede forudsætninger.
Konsekvens	For hver gruppe, karakteriseret ved rettigheder til at anvende en eller flere services eller applikationer, anslås volumen i gruppens aktiviteter, og hvilken variation over tid Folkekirkens It forventer i disse aktiviteter. Herudfra anslås, hvorledes Kirkenettets systemer forventes belastet.

22	PERFORMANCEKRAV TIL ALLE SERVICES OG APPLIKATIONER
Definition	Folkekirkens It opstiller konkrete performancekrav til alle sine services og applikationer. Performancekravene er **Svartid:** Fra brugeren aktiverer funktionen til resultatet er tilgængeligt for brugeren. **Driftstid:** Det tidsrum på døgnet, hvor servicen eller applikationen er tilgængelig. **Oppetid:** Den procentdel af åbningstiden, hvor servicen skal svare, og den andel af klienterne, som dette skal gælde for. **Retableringstid:** Den tid, der må gå, inden servicen eller systemet fungerer igen i tilfælde af nedbrud (katastrofe).
Begrundelse	For at sikre, dels at applikationerne fungerer tilfredsstillende i den daglige drift, dels for at sikre, at der er taget højde for retableringstiden i forbindelse med ikkeplanlagte hændelser.
Konsekvens	Mindstekravene for enhver service eller applikation i Kirkenettet skal overholdes. Krav vedrørende svartider, driftstid (tilgængelighed) og retableringstid skal leve op til Risikovurderingen.

1.5 Brugervenlighed og tilgængelighed

23	TILGÆNGELIGHED FOR ALLE
Definition	Kirkenettets websteder skal indrettes i overensstemmelse med de obligatoriske fællesoffentlige principper om tilgængelighed for alle.
Begrundelse	Kirkenettets websteder skal primært betjene ansatte og valgte, sekundært landets borgere og skal derfor i videst muligt omfang leve op til krav om tilgængelighed for alle.
Konsekvens	For websteder skal der ved design og funktionalitet sikres tilgængelighed for personer med funktionsnedsættelse. Hvor det ikke er muligt at gøre det fælles design og den fælles funktionalitet tilgængelig for alle, skal der indrettes særskilte faciliteter for personer med funktionsnedsættelse. Webstederne indrettes i overensstemmelse med *Standard for tilgængelighed* [WCAG - Web Content Accessibility Guidelines på niveau AA]

24	FOKUS PÅ BRUGERVENLIGHED
Definition	Ved udvikling af nye it-systemer og videreudvikling af eksisterende skal der være fokus på brugervenlighed
Begrundelse	Fokus på design af brugergrænsefladen og optimering heraf (GUI, UX etc.) vil sikre brugeren af systemet en væsentlig bedre oplevelse. Et brugervenligt design vil give færre kilder til fejl ved brug af systemet. Brugergrænsefladen er en mindst lige så væsentlig del af it-systemer som selve kodningen.
Konsekvens	Ved udvikling af nye systemer eller væsentlige ændringer i eksisterende systemer skal det sikres, at brugergrænsefladen får en optimal udforming. Dette skal ske i samarbejde med dels brugerne af systemet og dels kompetencer inden for brugervenlighed.

25	MÅLRETTEDE BRUGERFLADER
Definition	I Kirkenettet er brugerflader målrettet de brugergrupper, som anvender dem.
Begrundelse	Kirkenettet servicerer mange forskellige brugergrupper, og der skal både tages hensyn til brugervenlighed, effektivitet og ressourceforbrug i udviklingen.
Konsekvens	For hver brugergruppe skal Folkekirkens It karakterisere - hvilke typer brugerudstyr services skal kunne betjenes fra - om der skal tages hensyn til funktionshæmmede - hvilken indlæringskurve der er acceptabel - om der sker overholdelse af en eventuel designmanual.

26	FORENKLE OG HARMONISERE BRUGERFLADER
Definition	Folkekirkens It forenkler og harmoniserer brugerflader, så den enkelte bruger i højere grad oplever en ensartet it-arbejdsplads.
Begrundelse	For den enkelte bruger vil enkle og ensartede brugerflader på tværs af systemerne betyde mindre oplæring, en lettere arbejdssituation og større effektivitet. Særligt for brugere med begrænset anvendelse er enkelhed og overskuelighed afgørende.
Konsekvens	Applikationer indarbejdes i Den Digitale Arbejdsplads.

27	ENKELT OG SIKKERT LOG-IN
Definition	Log-in i Kirkenettet skal balanceres med krav om sikkerhed.
Begrundelse	På den ene side skal der arbejdes på, at man kun én gang skal logge på til mange systemer. På den anden side skal sikkerheden skærpes, i takt med at flere systemer er omfattet f.eks. med certifikat eller biometri.
Konsekvens	Der kan ikke arbejdes på enklere log-in, uden at der samtidig arbejdes på at fastholde eller forøge sikkerheden.