



By-, Land- og Kirkeministeriet
Folkekirken's It

STRATEGI FOR STYRING AF KIRKENETTET 2026-2028

December 2025

FIT-Akt id: 533875



Baggrund

Digitalisering i folkekirken sker i et samspil mellem overordnede målsætninger, teknologiske muligheder og konkrete beslutninger. Folkekirkens og By-, Land- og Kirkeministeriets digitaliseringsstrategi 2026-2030 udstikker strategisk retning for de næste fem års udvikling af digitale redskaber og rammer for kirkelige og administrative opgaver.

Digitaliseringsstrategien understøttes af en *Strategi for styring af Kirkenettet*, som med en treårig tidshorizont beskriver, hvilke teknologier, it-politikker og styringsmodeller Folkekirkens It vil anvende som grundlag for at levere og udvikle it-ydelser til folkekirken og ministeriet.

Strategi for styring af Kirkenettet lægger sig endvidere op ad de rammer, der er fastlagt i gældende it-arkitekturprincipper for Kirkenettet samt i informationssikkerhedspolitik og cirkulære om informationssikkerhed for By-, Land- og Kirkeministeriet og Den danske folkekirke.

Strategien medvirker desuden til at understøtte personregistrering som samfundsvigtig funktion samt de forretningskritiske processer i ministeriet og folkekirken.

Folkekirkens It er det kontor i By-, Land- og Kirkeministeriet, som varetager drift og udvikling af de fælles digitale løsninger på Kirkenettet. Som en del af ministeriet er Folkekirkens It underlagt de almindelige forvaltningsmæssige og statslige regler samt revision.

Kirkenettet dækker over programmer og services, som er etableret for By-, Land- og Kirkeministeriet og de folkekirkelige myndigheder. En bruger kan tilgå Kirkenettet fra en Kirkenet-pc, og et udvalg af services kan anvendes fra en ikke-Kirkenet-pc eller mobil enhed. En Kirkenet-pc er en sikkerhedshærdet pc med præinstallerede programmer, som leveres af Folkekirkens It.

Strategi for styring af Kirkenettet indeholder bl.a. rammer for valg af teknologi og anskaffelse af nye it-løsninger, og hvilken infrastruktur og arkitektur der arbejdes ud fra m.v. Strategien skal således sikre, at konkrete digitaliseringsinitiativer kan gennemføres med de mest hensigtsmæssige tekniske midler tillige med det rette niveau af sikkerhed og beskyttelse af personoplysninger.

Strategi for styring af Kirkenettet bidrager til optimal udnyttelse af de midler, der anvendes på it via en sammenhængende og veltilrettelagt styring, herunder effektiv anvendelse af eksterne leverandører samt rettidig vedligeholdelse og fornyelse af it-infrastrukturen.

Denne strategi er dermed Folkekirkens Its værktøj til at sikre fælles forståelse og konsistens i arbejdet vedrørende følgende temaer:

- Den anvendte it-arkitektur og -infrastruktur (afsnit 2)
- Den valgte arkitektur (afsnit 3)
- Den fastlagte informationssikkerhed og databeskyttelse (afsnit 4)
- Den valgte placering af opgaveløsningen, hhv. internt eller ved eksterne leverandører (afsnit 5)
- Den vedtagne styringsmodel for it og leverandører (afsnit 6).



1	Forudsætninger for strategien	4
2	It-målsætninger	5
2.1	Hvilken it-arkitektur er der brug for?	5
2.1.1	Behov afledt af digitaliseringsstrategien	5
2.2	Teknologier, der understøtter arkitekturen	5
2.2.1	Miljøer/platforme	6
2.2.2	Påvirkning af it-infrastrukturen	7
2.3	Udfasning af it-systemer	7
2.4	Arbejdspladsudstyr	7
3	Arkitekturvalg	8
3.1	Krav til udvikling	8
3.2	Brugerstyring	8
3.2.1	Brugere på Kirkenettet	8
3.2.2	Brugere med administrative rettigheder	9
3.3	Integrationsteknologier	9
3.4	Applikationer	9
3.4.1	Applikationer med integration i Folkekirken Its brugerstyring	9
3.4.2	Applikationer, der primært retter sig mod offentligt tilgængelige hjemmesider	9
4	Informationssikkerhed og databeskyttelse	10
4.1	Organisering	10
4.2	Sikkerhedsniveau og målsætninger	10
4.3	Styring og realisering af målsætning	11
4.4	Beredskab og kontrol	11
5	Hvilke opgaver løses internt henholdsvis eksternt?	12
5.1	Principper for anvendelse af interne og eksterne it-kompetencer i Folkekirken It	12
5.1.1	Interne kompetencer	12
5.1.2	Eksterne kompetencer	12
6	It-governance	13
6.1	Gennemførelse af it-projekter	13
6.2	Leverandørstyring	14



1 Forudsætninger for strategien

Digitale løsninger på Kirkenettet skal være robuste, løbende kunne opdateres, være stabile i drift, brugervenlige og velfungerende. Derfor baseres digitalisering i folkekirken som hovedregel på teknologier, der har en vis udbredelse, og på metoder, som er velafprøvede. Det gælder især for administrative systemer på områder, hvor folkekirkens behov er sammenlignelige med andre offentlige institutioners.

Folkekirkens It skal med andre ord ikke være 'first-mover' med hensyn til ny teknologi – men gerne være dem, der følger lige efter, hvor det giver teknologisk mening i forhold til den øvrige infrastruktur og gældende strategier, og hvor det bærende element er, at der direkte eller indirekte er en brugermæssig værdi at hente.

Strategi for styring af Kirkenettet (herefter Strategien) er Folkekirkens Its værktøj til at fastlægge rammer for anskaffelse af it-systemer, udvikling, styring og it-vedligehold samt udfasning af it-systemer således, at Kirkenettets it-systemportefølje til enhver tid bedst muligt understøtter By-, Land- og Kirkeministeriet og folkekirkens forretningsbehov og dermed skaber mest mulig værdi.

På baggrund af Strategien udarbejder og vedligeholder Folkekirkens It et teknisk roadmap, der for en treårig periode tydeliggør de nødvendige driftsmæssige initiativer, eksempelvis ved udløb af teknologier og standarder.

Det tekniske roadmap er til tjenstlig brug og indgår ikke i den offentliggjorte strategi.

Herudover vedligeholdes i forhold til digitaliseringsstrategien i en projektportefølje et overblik over igangværende projekter og initiativer samt en applikationsportefølje.

Projektporteføljen og applikationsporteføljen er sammenhængende, da færdige projektløsninger indgår i applikationsporteføljen ved projektafslutning. Omvendt kan idriftsatte applikationer afføde et behov for fornyelse eller større justeringer, der foranlediger igangsættelse af nyt projekt, som indgår i projektporteføljen.

Strategien godkendes af Folkekirkens Its ledelse og revideres som hovedregel årligt.



2 It-målsætninger

2.1 Hvilken it-arkitektur er der brug for?

2.1.1 Behov afledt af digitaliseringsstrategien

2.1.1.1 Grundlæggende it-arkitektur

For at kunne understøtte Digitaliseringsstrategien samt følge den teknologiske udvikling skal Folkekirkens It løbende kunne tilpasse arkitekturen på Kirkenettet og derfor konstant være opmærksom på alt, hvad der rører sig, og i hvilken retning udviklingen går.

I forbindelse med anskaffelse af enhver ny løsning skal der være en åben dialog således, at systemerne ikke risikerer uforvarende at blive afhængige af en bestemt teknologi eller udelukkende kan interagere med én type udstyr.

Der anvendes adskilte udviklings-, test- og produktionsmiljøer, og udvikling må ikke ske i test- og produktionsmiljøer. Test af nye systemer på testmiljøet skal sikre, at de nye systemer er kompatible med allerede eksisterende systemer inden idriftsættelse. Samtidig sikrer Folkekirkens It, at de nødvendige standarder er korrekt anvendte, at dokumentation er til stede, samt at løsningerne kan afvikles i et stabilt driftsmiljø.

I henhold til en risikovurdering etableres redundans på kritisk infrastruktur og udvalgte applikationer.

2.1.1.2 Fleksibel it-infrastruktur

Folkekirkens It skal levere en it-infrastruktur, der hurtigt og sikkert kan tilføjes ressourcer, når der opstår behov herfor. Ligeledes skal der sikkert og hensigtsmæssigt kunne lukkes for systemer, der ikke længere er i brug.

Det er vigtigt løbende at overveje fleksibilitetsbehov i forhold til systemer og bagvedliggende it-infrastruktur.

2.1.1.3 Økonomi og effektivitet

Ved valg af it-arkitektur anvendes en totaløkonomisk betragtning. Det analyseres, hvilken arkitektur og med hvilken fleksibilitet der skal udbydes services og til hvilke produkter. Analysen beror på parametre for tilgængelighed, sikkerhed, brugervenlighed samt hastighed som grundelementerne i valget af teknologi og leverandør.

På denne baggrund vælges den arkitektur, som samlet set vurderes økonomisk mest fordelagtig, når der tages højde for ovennævnte parametre samt de medarbejderressourcer, der skal anvendes til udvikling, implementering, drift og vedligeholdelse af arkitekturen.

2.2 Teknologier, der understøtter arkitekturen

På baggrund af ovenstående mål for it-arkitekturen anvender Folkekirkens It den it-infrastruktur, som beskrives i det følgende.



2.2.1 Miljøer/platforme

For at sikre en stabil og samtidig fleksibel drift af it på Kirkenettet leverer Folkekirkens It primært it på virtuelle servere placeret hos Kirkenettets driftsleverandør. Dette suppleres af løsninger hostet hos applikations- og cloudleverandører.

2.2.1.1 Patchning og opdatering på servere

Der foretages fast månedlig patchning på Kirkenettets servere. Derudover patches og opdateres løbende baseret på overvågning af de enkelte servere og disses status.

Operativsystemer (OS) på servere anvendes i to versioner bagud. En ny version af et OS anvendes først, når den første samlede opdatering foreligger (update 1). Der vil derfor være en kontinuerlig proces med opgradering af servere, der sikrer, at gamle versioner løftes til den seneste godkendte version. Dette vil i perioder medføre, at der kan eksistere op til tre samtidige OS-versioner.

Der anvendes Windows som OS på alle servere i Kirkenettet på nær til hjemmesideservere (se AWS nedenfor), hvor der anvendes en LAMP-konfiguration.

2.2.1.2 Microsoft cloudservices

På Kirkenettet anvendes en række Microsoft cloudservices, herunder Microsoft 365, Azure og Entra, i et hybridt setup.

Folkekirkens It vælger mellem Platform as a service (PaaS), Infrastruktur as a service (IaaS) og Software as a service (SaaS)¹ ud fra en samlet vurdering af den mest hensigtsmæssige løsning både økonomisk og infrastruktur-mæssigt.

Azure anvendes til løsninger, hvor der er behov for løbende at op- og nedskalere kapaciteten, eks. Valgsystemet til understøttelse af menighedsrådsvalg, samt til testmiljøer. Azure giver desuden mulighed for at kunne lukke ned, når systemer og miljøer ikke anvendes.

Endvidere benyttes Azure til anvendelse og administration af Office365.

2.2.1.3 Amazon Web Services

I Amazon Web Services (AWS) er de offentligt tilgængelige hjemmesider og enkelte systemer placeret. Der benyttes hovedsageligt IAAS-løsninger i AWS.

Hjemmesiderne er med placeringen i AWS adskilt fra den øvrige del af Kirkenettet. Dermed minimeres skaden, såfremt hjemmesiderne rammes af angreb.

Den daglige drift af AWS-løsningen varetages af en ekstern part, der sørger for patching af de dele, som AWS ikke varetager. Herudover er den eksterne part ansvarlig for backup og overvågning samt den tekniske dialog med AWS.

2.2.1.4 Sikkerhedsforanstaltninger

Kirkenet-pc'er, der anvendes på Kirkenettet, bliver godkendt via de på pc'en aktiverede sikkerhedspolitikker.

¹ De forskellige services er nærmere beskrevet i Digitaliseringsstyrelsens Vejledning i anvendelse af cloudservices (juli 2020). Vejledningen ses [her](#).



Ved hjælp af en VPN-forbindelse skabes automatisk en krypteret adgang til Kirkenettet fra Kirkenet-pc'en. Der stilles krav om anvendelse af flerfaktor autentificering ved brug af VPN.

På Kirkenettet er der etableret foranstaltninger (firewall, conditional access regler, antivirus, logning, SOC m.v.), som beskytter al data, der går ind til og ud fra Kirkenettet.

2.2.2 Påvirkning af it-infrastrukturen

For at sikre et stabilt og sikkert miljø på Kirkenettet vedligeholder Folkekirkens It et overblik over tidspunkter for, hvornår hardware og software (OS, Office-pakke m.v.) skal udskiftes.

Dette overblik fremgår af det tekniske roadmap, som løbende revideres.

2.3 Udfasning af it-systemer

Det skal sikres, at it-systemer udfases forsvarligt og korrekt, herunder at data håndteres i overensstemmelse med gældende lovgivning, at aflevering sker til Rigsarkivet i henhold til evt. foretagens anmeldelse, og at udgifter til it-systemet ophører.

Folkekirkens It skal sammen med berørte leverandører bistå den forretningsmæssige systemejer med at udarbejde en plan for nødvendige aktiviteter ved udfasning af et it-system.

I overensstemmelse med indgået databehandleraftale vil data behandlet af en leverandør enten blive slettet helt eller blive tilbageleveret ved udfasning af et it-system og ophør af behandlingsaktiviteter i forbindelse med personoplysninger.

2.4 Arbejdspladsudstyr

Pc'er og særligt udstyr som attestprintere, der skal tilkobles Kirkenettet, skal altid anskaffes gennem Folkekirkens It. Øvrigt udstyr kan i nogle tilfælde anskaffes gennem Folkekirkens It, men også købes hos andre leverandører, eks. multifunktionsprintere.

I udgangspunktet tilbyder Folkekirkens It følgende typer af udstyr:

- Bærbare pc'er
- Printere
- Andet tilbehør til en it-arbejdsplads, eks. skærme, mus/tastatur, udstyr til videomøder m.v.

Udstyr købes via Kirkenettets bestillingsside. Inden køb kan foretages, skal institutionen have indgået en drifts- og indkøbsaftale med Folkekirkens It.

Smartphones og tablets kan ikke anskaffes gennem Folkekirkens It.



3 Arkitekturvalg

3.1 Krav til udvikling

Ved udviklingen af applikationer til Kirkenettet skal gældende standarder for tilgængelighed, sikkerhed, brugervenlighed samt hastighed og grafisk konsistens i forhold til brugerfladen overholdes.

Som udgangspunkt skal applikationer kunne anvendes på den type udstyr, som brugeren foretrækker i den givne situation. Dvs., at løsningerne i videst muligt omfang skal være responsive og derved kunne tilpasse sig brugerinteraktionen, så de kan benyttes både på en pc og en mobil enhed. Således sikres den maksimale brugervenlighed i brugen af applikationen.

Udvikling skal ske efter principper, som sikrer god databeskyttelse, hvilket vil sige databeskyttelse gennem design (privacy by design) og databeskyttelse gennem standardindstillinger (privacy by default). Dette skal bl.a. sikre, at anvendelse af personoplysninger minimeres, og at der i nødvendigt omfang anvendes anonymisering, pseudonymisering, kryptering af data, korte opbevaringsperioder og begrænset adgang til data, jf. Vejledning om Behandlingssikkerhed og Databeskyttelse gennem design og standardindstillinger (Juni 2018).²

3.2 Brugerstyring

3.2.1 Brugere på Kirkenettet

Brugeradministrationen i Kirkenettet er baseret på informationer fra Kirkenettets Informationssystem (KIS), som indeholder masterdata (stamoplysninger) på sogne, menighedsråd, folkekirkens og By-, Land- og Kirkeministeriets personale m.v. Den aktive styring af rettigheder (adgang) til informationer, portaler, filer m.m. sker gennem AD/Entra ID.

Oven på AD ligger der en brugeradministrationsløsning baseret på Microsoft Identity Manager (MIM) således, at Kirkenettets sikkerhedsansvarlige selv skal håndtere administrationen af deres egne Kirkenetbrugere.

På Folkekirkensintranet.dk findes en løsning til administration af udvalgsbrugeres³ rettigheder og adgange. Løsningen er udviklet som en del af Kirkeportalen og ligger i en Microsoft teknologistak.

Brugerstyringen skal - hvor det er muligt - ske via ovennævnte systemer, som nedsætter ekspeditionstiden og minimerer risikoen for menneskelige fejl.

Som udgangspunkt skal systemer i Kirkenettet kunne integreres med AD. På den måde sikres det, at administrationen af adgangen til systemer sker via de dertil oprettede brugergrupper og inden for de krav til single-sign-on, som er fastlagt i it-

² Vejledningen ses på [Datatilsynets hjemmeside](#) under Vejledninger.

³ Udvalgsbrugere er menighedsråds- og provstiudvalgsmedlemmer samt øvrige eksterne brugere med tilknytning til menighedsrådet.



arkitekturprincipperne. Dette gælder også for løsninger hostet af applikationsleverandører.

3.2.2 Brugere med administrative rettigheder

Styring af leverandørers og Folkekirken Its adgang til servere og services på Kirkenettet sker med Microsoft-værktøjet Privileged Identity Management (PIM). Der tillades kun adgang med unikke brugere, og al aktivering af rettigheder logges. Brugere skal være oprettet i MIM, før de kan få adgang via PIM, og ved indlogging kræves brug af multifaktorgodkendelse.

Adgang kan kun opnås i et begrænset tidsrum, og enhver anmodning om adgang skal være begrundet.

3.3 Integrationsteknologier

Som udgangspunkt benyttes der altid en anerkendt standard til udveksling af data mellem de forskellige systemer, interne som eksterne. Det betyder bl.a., at de systemer, som Folkekirken It stiller til rådighed, i muligt omfang skal udstille relevante snitflader (API'er) efter alment anerkendte standarder.

Integrationsmuligheder er nærmere beskrevet i it-arkitekturprincipperne.

3.4 Applikationer

Applikationer til Kirkenettet skal af hensyn til videreudvikling, vedligeholdelse og kvalitet være standard- og/eller rammesystemer så vidt muligt. Det vil som hovedregel også sikre det bedste forhold mellem pris og kvalitet. Det betyder, at systemudvikling, som omfatter mere end konfiguration, begrænses.

I visse tilfælde vil folkekirkens særlige struktur og opgaver dog kræve løsninger, som designs og udvikles specifikt til folkekirken.

Applikationer anskaffes som hovedregel med tilhørende vedligeholdelses- og opgraderingsaftaler. Overblik over applikationer fremgår af applikationsporteføljen.

Når der sker systemudvikling, skal nedenstående krav overholdes.

3.4.1 Applikationer med integration i Folkekirken Its brugerstyring

Applikationer, der har behov for at integrere med Folkekirken Its brugerstyring, skal udvikles på Microsoft-teknologier. Til dette benyttes primært MS SQL som database, og IIS benyttes som webserver.

3.4.2 Applikationer, der primært retter sig mod offentligt tilgængelige hjemmesider

De offentligt tilgængelige hjemmesider udvikles i et open source Content Management System, enten i TYPO3 eller NEOS. Disse programmer implementeres på en server konfigureret med Linux/MySQL/PHP.



4 Informationssikkerhed og databeskyttelse

De specifikke retningslinjer, der skal sikre fortrolighed, integritet, tilgængelighed og autenticitet gældende for applikationer og data, er fastlagt i og reguleret af Informationssikkerhedspolitik for By-, Land- og Kirkeministeriet og Den danske folkekirke samt Cirkulære om informationssikkerhed og persondatabeskyttelse for By-, Land- og Kirkeministeriet og den danske folkekirke.

Politikken og cirkulæret er udarbejdet i henhold til den gældende statslige sikkerhedsstandard, ISO 27001:2022, samt databeskyttelseslovgivningen⁴ og gældende statslige vejledninger om informationssikkerhed og databeskyttelse.

4.1 Organisering

For By-, Land- og Kirkeministeriet og folkekirken er der udpeget en databeskyttelsesrådgiver og en informationssikkerhedskoordinator, som har fokus på databeskyttelse og informationssikkerhed.

Der er desuden nedsat et informationssikkerhedsudvalg for ministeriet og folkekirken, som består af repræsentanter fra ledelse og medarbejdere i departement og stiftsadministrationer samt repræsentanter fra en række folkekirkelige organisationer. Souschefen for Folkekirkens It er formand for informationssikkerhedsudvalget, mens informationssikkerhedskoordinatoren varetager sekretariatsbetjening af udvalget.

Det forretningsmæssige ansvar er forankret ved system- og dataejere, som ved behandling af personoplysninger endvidere vil være dataansvarlige. Systemejerne bistås af de tekniske systemansvarlige i Folkekirkens It.

I det daglige træffes dispositioner og afgørelser af Folkekirkens Its ledelse, og disse afgørelser effektueres umiddelbart af IT-drift og Sikkerhedsenheden, bestående af informationssikkerhedskoordinator, drifts- og sikkerhedsmedarbejdere.

Fordeling af roller, ansvar og beføjelser vedrørende informationssikkerhed og databeskyttelse er beskrevet i ledelsessystem for By-, Land- og Kirkeministeriet.

4.2 Sikkerhedsniveau og målsætninger

Folkekirkens brug af digitale løsninger skal ske på en tryk og sikker måde, som fastholder den høje tillid, som samfundet har til folkekirken. Folkekirkens mange myndigheder og institutioner skal overholde databeskyttelseslovgivningen og gældende cyber- og informationssikkerhedsstandarder og -krav.

Et højt digitalt sikkerhedsniveau opnås med en kombination af sikre systemer og sikker adfærd. Folkekirkens It sikrer løbende, at Kirkenettets systemer overholder de gældende sikkerheds- og databeskyttelsesstandarder. Det er samtidig et væsentligt

⁴ Databeskyttelsesforordningen (Europa-Parlamentet og rådets forordning (EU) 2016/679 af 27. april 2016) samt Databeskyttelsesloven (LOV nr. 502 af 23/05/2018).



hensyn ved udvikling af nye digitale løsninger, at sikkerhed tænkes ind fra starten, således at brugervenlighed og sikker adfærd indgår i løsningsdesignet.

Sikkerhedsniveauet på Kirkenettet er fastlagt ud fra en risikobaseret tilgang og er beskrevet nærmere i informationssikkerhedspolitikken. Den risikobaserede tilgang betyder, at der er fokus på driften af de mest forretningskritiske processer og it-aktiver samtidig med, at der også er den nødvendige sikkerhed for øvrige processer og aktiver. Der skal implementeres de sikkerhedsforanstaltninger på Kirkenettet, der er nødvendige for at opretholde sikkerhedsniveauet i forhold til det aktuelle trusselsbillede.

Viser en risikovurdering, at sandsynligheden for en sikkerhedshændelse er højere end middel, skal Folkekirkens It – under hensyntagen til de økonomiske forhold og efter aftale med systemejeren – implementere sikkerhedsforanstaltninger til at nedbringe sandsynligheden og dermed den samlede risiko. Såfremt konsekvensen ved en forretningskritisk proces er høj eller meget høj, skal sandsynligheden for og/eller konsekvensen ved en hændelse på tilsvarende måde søges bragt ned på lav.

4.3 Styring og realisering af målsætning

Til styring af arbejdet med informationssikkerhed og databeskyttelse, herunder gennemførelse af risikoanalyser, anvendes værktøjer anbefalet af Statens netværk for informationssikkerhed, Digitaliseringsstyrelsen, Ministeriet for samfundssikkerhed og beredskab samt Styrelsen for Samfundssikkerhed.

Folkekirkens It, herunder særligt informationssikkerhedskoordinatoren, deltager i relevante fora, uddannelser, konferencer m.v. for at sikre, at den fornødne sikkerhedsmæssige viden er til stede for at kunne opretholde et højt sikkerhedsniveau på Kirkenettet.

Ved anskaffelse af nye it-systemer samt ved væsentlige ændringer skal der altid foretages en risikovurdering og evt. en konsekvensanalyse.

En systematisk risikovurdering af forretningskritiske processer og de tilhørende it-aktiver foretages årligt, og på baggrund heraf fastlægges behovet for evt. yderligere sikringsforanstaltninger.

Sikkerhedsenheden i Folkekirkens It gennemfører jævnligt informationskampagner og lignende aktiviteter for at øge bevidstheden om informationssikkerhed og databeskyttelse på Kirkenettet og gældende retningslinjer samt for at skærpe bevidstheden om eget ansvar for opretholdelse heraf.

4.4 Beredskab og kontrol

Det er Folkekirkens Its ansvar, at der foreligger systemmæssige retableringsplaner, og at disse afprøves løbende for at sikre aktualitet, både i forhold til restore af data og gendannelse af it-systemer.

De forretningsmæssige systemejere er ansvarlige for at udarbejde og vedligeholde nødplaner i tilfælde af manglende it-understøttelse.

Gennem tilbagevendende it-sikkerhedsreviews, kontroller og audits sikrer Folkekirkens It den fortsatte overholdelse af gældende standarder og regler.



5 Hvilke opgaver løses internt henholdsvis eksternt?

It-ydelser til Kirkenettet leveres både af Folkekirken It og eksterne it-leverandører.

I det følgende beskrives de principper, der fastlægger, hvilke it-kompetencer og hvilken opgaveløsning det er nødvendigt at have internt i Folkekirken It, samt hvilke kompetencer og hvilke typer opgaver der vil blive indkøbt efter behov.

5.1 Principper for anvendelse af interne og eksterne it-kompetencer i Folkekirken It

Valget af, hvorvidt en given opgave ved Folkekirken It skal varetages internt eller eksternt, baseres på følgende overordnede princip:

- Opgaver skal løses fagligt forsvarligt og med den lavest mulige omkostning, samtidig med at Folkekirken It sikres leverancesikkerhed samt reel mulighed for styre og kontrollere de it-ydelser, der leveres til slutbrugerne.

5.1.1 Interne kompetencer

Folkekirken It vil internt opretholde kompetencer til opgaver, hvor:

- Der kræves stort kendskab til Kirkenettets brugere og dyb viden om arbejdsprocesser.
- Der forudsættes intern varetagelse for at sikre nødvendig styring og kontrol med de leverede it-ydelser, f.eks. projekt- og leverandørstyring samt sikring af persondata.

Opgaver, der primært løses internt, er arbejdet med strategi og governance vedrørende Kirkenettet, sikkerhed og databeskyttelse, herunder opfølgning på compliancestatus, supporthåndtering og herunder vejledning, uddannelse m.v.

Efter behov kan den interne opgavevaretagelse suppleres med ekstern bistand.

5.1.2 Eksterne kompetencer

Folkekirken It vil indkøbe ekstern bistand til opgaver kendetegnet ved:

- Specialistopgaver, hvor Folkekirken Its størrelse ikke giver kritisk masse til at opretholde den nødvendige kompetence.
- Standardopgaver, som kan indkøbes billigere end ved intern produktion.
- Adgang til skalérbare ressourcer med periodisk behov for bistand.

Opgaver, der typisk søges ekstern bistand til, er vurdering af sikkerheds- og driftsmæssige problemstillinger, juridisk og ledelsesmæssig rådgivning samt udvikling af applikationer. Dertil kommer de forretningskritiske ydelser, der leveres af eksterne it-leverandører inden for flerårige aftaler, herunder drift af store it-systemer som ESDH og løn samt drift af servere.



6 It-governance

It-governance handler om tilrettelæggelsen af arbejdet med it og digitalisering, særligt når det gælder ansvar, ledelse og organisering. De grundlæggende retningslinjer for it-governance i folkekirken er fastlagt af kirkeministeren i 2017, og omfatter fem hovedprincipper:

1. By-, Land- og Kirkeministeriet har ansvaret for Folkekirken It
2. It-Følgegruppen rådgiver om strategiske it-spørgsmål
3. Brugere inddrages fra først til sidst
4. Folkekirken tager ejerskab for de digitale løsninger
5. Digitale løsninger skal kunne betale sig.

Dette udmønter sig i forhold til Folkekirken Its daglige arbejde i den tilbagevendende gennemførelse af konkrete styringsaktiviteter, eks. vedrørende sikkerhed og databeskyttelse, men også vedrørende gennemførelse af projekter og leverandørstyring.

6.1 Gennemførelse af it-projekter

Når projekter helt eller delvist finansieres af fællesfonden er det et krav, at dette sker i henhold til *Retningslinjer for organisering og styring af it-projekter*.

Retningslinjerne bygger på statens it-projekt⁵- og programmodeller⁶ samt Økonomistyrelsens vejledninger om it-udviklingsprojekter⁷.

Formålet med retningslinjerne er dels at fastlægge de overordnede rammer og principper for organisering og styring og dels at beskrive, hvordan de udmøntes i praksis, herunder opliste de obligatoriske styringsdokumenter, som skal fastholde målsætningen om, at it-projekter forankres i forretningen og herudover sikre, at:

1. Det er tydeligt, hvordan og af hvem beslutninger træffes
2. Der i hele projektperioden sker en løbende opfølgning til projektets styregruppe
3. Alle omkostninger til et projekt opgøres.

Som en del af det samlede projektgrundlag skal fremgå, hvilke og hvor mange ressourcer organisationen skal bidrage med i udviklingsfasen, hvilke behov der er for at ændre i eksisterende arbejdsgange, samt hvordan organisationens brugere uddannes og trænes.

I forbindelse med større projekter sikres brugerne indflydelse på det færdige resultat ved nedsættelse af en bruger- og/eller referencegruppe.

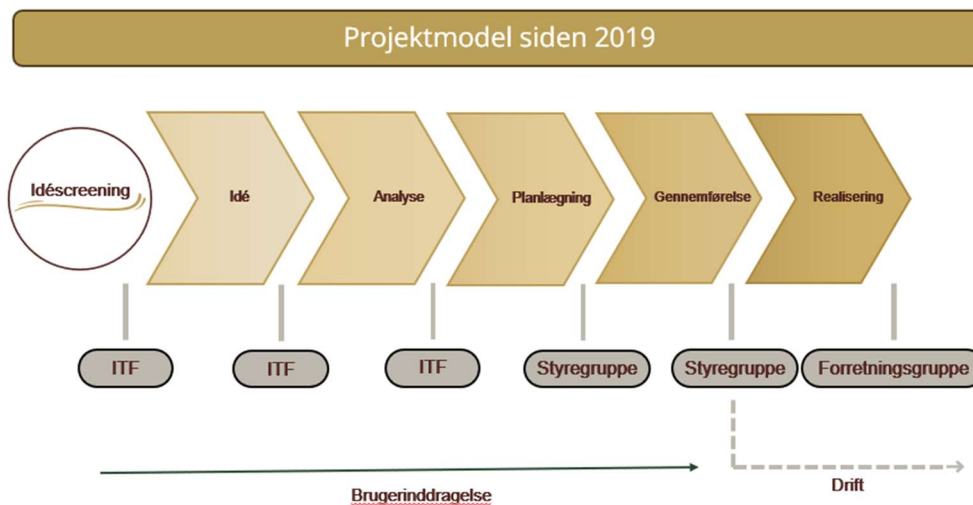
Projektmodellens faser er; Idé, Analyse, Planlægning, Gennemførelse og Realisering.

I projektforsløbets idéfase skal informationssikkerhedskoordinator og databeskyttelsesrådgiver inddrages med henblik på at sikre forankring og overholdelse af de informationssikkerheds- og databeskyttelsesmæssige retningslinjer og principper i projektet.

⁵ Vejledning til statens it-projektmodel, Digitaliseringsstyrelsen 2019

⁶ Vejledning til den fællesstatslige programmodel, Digitaliseringsstyrelsen 2016

⁷ Økonomistyrelsens vejledning om it-udviklingsprojekter



Forretningsudviklingsprojekter og driftsudviklingsprojekter i Folkekirkens It følger samme projektforsløb. Forretningsudviklingsprojekter forelægges It-Følgegruppen, mens driftsudviklingsprojekter som hovedregel ikke forelægges for It-Følgegruppen, men derimod for Folkekirkens Its ledelse.

For hvert projekt vurderes det, hvorvidt det er vandfaldsmodellen eller agil udvikling som udviklingsmetode, der skal anvendes. Uanset valget anvendes traditionel projektledelse som styringsredskab for tid, kvalitet, økonomi samt varetægelse af interessenter og styring af risici. I praksis vil Folkekirkens It typisk anvende en blanding af udviklingsmetoder, jf. også scenarier i Statens It-projektmodel.

Det tilstræbes, at initiativet og ansvaret for nye digitale løsninger og videreudvikling af eksisterende systemer i videst muligt omfang skal forankres hos systemejerne og dermed det sted i ministeriet og/eller folkekirken, som skal drage nytte af et system.

Derfor sidder den relevante enhed i ministeriet og/eller folkekirken med som projektejer, når der skal formuleres krav og specifikationer for en digitale løsning, når den konkrete løsning skal vælges, og når fordele, ulemper og gevinster skal vurderes.

6.2 Leverandørstyring

Ansvaret for leverandørstyring er forankret hos ledelse og systemansvarlige i Folkekirkens It. Den systemansvarlige skal sikre, at indgåede kontrakter overholdes, og at der leveres den i kontrakten aftalte dokumentation, herunder revisionserklæringer, SLA-rapportering, systemdokumentation m.v.

Med leverandører til forretningskritiske systemer holdes som minimum kvartalsvise forretnings-/styregruppemøder.

Ved kontraktindgåelse gennemfører den systemansvarlige en risikovurdering af både systemet og leverandøren. Risikovurderingen afgør det nødvendige tilsynsbehov, og systemansvarlig har ansvaret for at udføre tilsynet. Tilsynsbehovet kan revurderes på



baggrund af den årlige risikovurdering af systemet. Tilsyn med leverandører udføres i overensstemmelse med Datatilsynets vejledning om tilsyn med databehandlere⁸.

⁸ [Vejledning om tilsyn med databehandlere oktober 2021](#)