

Open source i den offent- lige sektor



Indhold

1. Introduktion.....	3
2. Resume	4
3. Hvad er open source-software?.....	5
3.1 Open source-software i desktop- og serverlaget.....	6
3.2 Udvikling og styring af open source-software	7
3.3 Inbound eller outbound open source-software	9
3.4 Sikkerhedsaspekter i open source-software	9
4. Rammer for anvendelse af open source-software.....	12
5. Danske myndigheders erfaringer	14
5.1 Myndighedernes erfaringer.....	14
5.2 Danske OSPO'er: OS2 og 4S	20
6. Tre danske cases	23
6.1 Sundhedsvæsenets Nationale Serviceplatform.....	23
6.2 OS2 - Et fællesoffentligt samarbejde om digital udvikling.....	24
6.3 Domstolsstyrelsens straffe- og skifteprogram.....	25
7. Internationale erfaringer.....	27
7.1 Erfaringer fra andre lande.....	27
7.2 Tiltag fra EU og FN	31
8. Forudsætninger.....	33
8.1 Organisation og implementering	33
8.2 Support og vedligeholdelse	35
8.3 Sikkerhed	36
8.4 Licensstyring og anskaffelse	38
8.5 Integration til anden software	39
8.6 Økonomi	40
8.7 Opsamling	42

1. Introduktion

I forbindelse med indgåelsen af "Aftale om ambitiøs og ansvarlig strategi for Danmarks digitale udvikling" (Digitaliseringsstrategien) mellem regeringen og Socialistisk Folkeparti, Liberal Alliance, Danmarksdemokraterne, Det Konservative Folkeparti, Enhedslisten, Radikale Venstre, Dansk Folkeparti og Alternativet i februar 2024, var der enighed om at igangsætte en analyse af open source i den offentlige sektor, herunder forudsætninger for anvendelsen¹

Open source-software adskiller sig fra proprietær software ved, at kildekoden er frit tilgængelig. Det kan give offentlige myndigheder, virksomheder, organisationer og privatpersoner mulighed for at tilgå, tilpasse og videreudvikle software efter egne behov samtidig med, at de potentielt kan opnå større uafhængighed af specifikke produkter og it-leverandører. Det betyder dog ikke, at open source-software nødvendigvis er gratis at anvende. Tværtimod kræver det ofte investeringer i kompetencer, implementering, vedligeholdelse, sikkerhedsforanstaltninger og lignende, som ofte er en del af pakken, når der indkøbes proprietær software.

I denne rapport undersøges det, hvordan open source-software anvendes blandt offentlige myndigheder i Danmark og hvilke overvejelser og strategier, der knytter sig til denne anvendelse. Det skal give et indblik i offentlige myndigheders tilgang til og oplevelse af open source-software som helhed.

Dernæst undersøges det hvilke tiltag, der arbejdes med internationalt og hvilke erfaringer, der er gjort med open source-software i andre lande.

Endeligt samler rapporten op på hvilke forudsætninger, der er for anvendelsen af open source-software i den offentlige sektor og perspektiverer til tiltag baseret på erfaringer fra Danmark og udlandet.

¹ [Aftale om en ambitiøs og ansvarlig strategi for Danmarks digitale udvikling](#)

2. Resume

Danske myndigheder anvender open source-software til mange formål og i meget varierende omfang. Open source-software er både applikationer til slutbrugeren som fx LibreOffice, Linux-styresystemer og Firefox-browseren. Men det indgår også dybere i teknologilagene, der driver og forbinder digitale tjenester eller som støtte- og servicekomponenter, der fungerer som en del af it-udvikleres værktøjskasse. Mens nogle myndigheder har en strategi om at anvende open source-software i større eller mindre omfang, vælger andre det, når det vurderes som det bedste valg i den konkrete situation. Kun få myndigheder bidrager til udvikling af open source-løsninger, som andre kan videreanvende, og hvis de gør, sker det oftest gennem fællesskaber som OS2.

Flere af de interviewede myndigheder kan se et potentiale for yderligere anvendelse af open source-software på udvalgte områder fx med henblik på øget genbrug af kode mellem myndigheder. De vurderer dog, at der er en række afhængigheder til proprietær software, og at de ofte mangler ressourcerne til at prioritere midler til deling af software. Myndighederne fremhæver derudover, at robusthed, regelmæssige tests og aktiv vedligeholdelse er afgørende for sikkerheden i både proprietær og open source-kode.

Andre landes erfaringer med og tilgange til open source-software er ligeledes forskellige. Mens nogle lande ikke har taget aktiv stilling til anvendelsen af og bidrag til open source-software, har andre fastsat principper og krav om, at offentlig egenudviklet software i udgangspunktet skal være open source. Det gælder fx Schweiz, Frankrig, Italien og Nederlandene. Der er kun få lande, der har gennemført egentlig gennemgribende implementering af open source-software i deres offentlige sektor. Flere EU-lande som Nederlandene, Frankrig og Tyskland, herunder delstaten Slesvig-Holsten, har dog for nylig iværksat en række større open source-tiltag særligt inden for desktop-software såsom kontorpakker. Det er dog vigtigt at bemærke, at den danske offentlige sektor er en af de mest digitaliserede i verden, og at andre landes tilgange og erfaringer derfor ikke nødvendigvis er sammenlignelige med en dansk kontekst.

Forudsætningerne for anvendelse af open source-software i den offentlige sektor varierer betydeligt afhængigt af både typen af software og formålet med anvendelsen. De eksisterende erfaringer fra Danmark og udlandet viser, at der generelt set må forventes omkostninger, når ny software tages i brug. Det gælder både i form af tekniske tilpasninger, men der kan også være tale om organisatoriske og kompetencemæssige tilpasninger. I nogle tilfælde skal myndigheden tage større ansvar for den anvendte it-løsning, hvis de vælger at anvende open source-software frem for at købe proprietær software af en leverandør. Det gælder fx, at myndigheden i højere grad skal have styr på licensvilkår, sikkerhedsopdateringer, fejl, support og vedligeholdelse af softwaren. Der findes en række eksempler på, hvordan myndigheder i Danmark og udlandet har håndteret disse forudsætninger enten alene eller i samarbejde med andre myndigheder. I andre tilfælde stilles open source-løsningen til rådighed af en organisation eller en privat leverandør, og her stilles der ikke nødvendigvis højere krav til myndigheden end ved proprietær software. Det er også vigtigt at være opmærksom på, at der er nogle systemer som er underlagt særlige rammer, fx kritisk infrastruktur, som gør, at det ikke er hensigtsmæssigt at offentliggøre som open source-software i sin helhed.

3. Hvad er open source-software?

Begrebet open source er oprindeligt forbundet med software eller kildekode. Imidlertid har begrebet i de seneste år udviklet sig og kan nu også bruges om fx hardware, data, undervisningsmaterialer og design, hvor åbenheden relaterer sig til fx tekniske tegninger, datafiler eller videndeling. Denne udvidelse af open source-begrebet medfører en øget kompleksitet, da principperne om åbenhed og deling anvendes inden for vidt forskellige domæner, hvor der langt fra er enighed om forudsætninger og definitioner. I denne rapport foretages derfor en afgrænsning, således, at der alene fokuseres på open source-software.

Open source-software er software udgivet under en licens, der giver enhver ret til at bruge, undersøge, ændre og dele softwaren frit og til ethvert formål.²

Open source-software står dermed definitions-mæssigt i modsætning til proprietær software, der er ejet af fx en person, virksomhed eller organisation, der har ret til at bestemme over softwarens brug og udvikling. I praksis fungerer de to dog ofte i samspil, da open source-komponenter indgår i næsten al proprietær software.

For at forstå muligheder og begrænsninger i anvendelsen af open source-software, er det vigtigt at kende de overordnede licenstyper, der derfor gennemgås i følgende tabel.

Tabel 1. Open source- og proprietære licenser

Licenstype	Hovedtræk
Open source – Copyleft	Copyleft-licenser har til formål at sikre, at softwaren forbliver åben – også hvis andre anvendere vælger at videreudvikle eller tilpasse koden. Hvis en myndighed, virksomhed eller andre ønsker at dele den tilpassede software, skal det ske under samme licens. Der findes både stærke og svage copyleft-licenser: • Stærk copyleft: Hele it-systemet, som open source-softwaren er en del af, skal gøres åbent, hvis open source-softwaren anvendes. En myndighed eller it-leverandør kan derfor ikke blande softwaren ind i proprietær kode uden at åbne hele koden for offentligheden, hvis softwaren videredistribueres. • Svag copyleft: Kun den konkrete open source-software skal forblive åben, mens resten af it-systemet kan have andre licenser, hvis softwaren videredistribueres.
Open source - Permissive	Permissive licenser giver myndigheder, it-leverandører og andre større handle- rum. Softwaren kan i de fleste tilfælde anvendes og videredistribueres efter eget ønske, herunder indgå i proprietær software, så længe ophavsret og ansvarsfraskrivelser beskrevet i licensen følges.
Proprietær licens	Ved proprietære licenser er brug, ændring og videredistribution af softwaren be- grænset til leverandørens vilkår.



² [Vejledning om brug af open source i den offentlige sektor | Fællesoffentlig Digital Arkitektur](#). Open source er et omstridt begreb, og der findes flere forskellige definitioner. Definitionen fra Open Source Initiative er en af de mest udbredte: [The Open Source Definition – Open Source Initiative](#). Til formålet i denne rapport vurderes ovenstående definition dog at være tilstrækkelig.

I den brede offentlighed kendes open source-software primært gennem applikationer som LibreOffice, Linux, Mozilla-produkter og lignende programmer, som kan downloades og anvendes gratis af slutbrugere. Der kan således være en tendens til at forveksle open source-software med gratis software (free-ware). Gratis software er dog ikke nødvendigvis åbent og tilgængeligt for tilpasninger og ændringer. Tilsvarende kan det være forbundet med andre bindinger, som giver lukrative forhold for softwarens ejer – fx adgang til brugerdata, som kan sælges videre, reklamer, som brugeren eksponeres for, eller en vej til mersalg af nye betalingspålagte produkter. Så selv om open source-software licenser er gratis, er det ikke al gratis software, der er open source.

Derudover er der mange former for open source-software, der ikke er rettet mod slutbrugeren. Open source-software indgår mange forskellige steder i offentlige myndigheders it-løsninger. Dertil kommer, at der er meget stor forskel på, hvem der udvikler og styrer softwaren og derved sikrer, at den fx er løbende opdateret og sikker. Endeligt kan der være en forskel på, om myndigheder og andre organisationer alene anvender open source-software (inbound), eller om de også bidrager med open source-software, som andre kan anvende (outbound). Formålet med dette kapitel er at introducere disse centrale nuancer i forståelsen af open source-software.

3.1 Open source-software i desktop- og serverlaget

Open source-komponenter spiller en central rolle i alle lag af den moderne teknologistak, også i den danske offentlige sektor. Open source-software kan både indgå i desktoplaget, hvilket vil sige den brugergrænseflade, der møder brugeren, og i serverlaget, som er de underliggende tekniske lag, der driver og forbinder digitale tjenester. Herunder præsenteres eksempler på forskellige typer af open source-software opdelt i de to områder, for at vise spændvidden i anvendelsen.

Tabel 2. Eksempler på open source-software i desktop- og serverlaget

 Desktoplaget Desktoplaget dækker over de komponenter i it-infrastrukturen, der anvendes direkte af brugeren. Det inkluderer både operativsystem, brugerflade og applikationer.	
Browsere og rendering engines	Mange browsere er stillet til rådighed som open source-software. Fx er Mozilla Firefox en open source-browser, mens Chrome og Edge er baseret på open source-renderingmotoren <i>Chromium</i> .
Desktopmiljøer og applikationer	Open source-kontorpakker som <i>LibreOffice</i> og e-mailklienten <i>Thunderbird</i> anvendes i stigende grad. Open source-operativsystemer som <i>Ubuntu</i> , <i>Debian</i> og <i>Fedora</i> tilbyder fuldt udstyrede desktopmiljøer.



Serverlaget

Serverlaget udgør den tekniske rygrad, der sikrer, at digitale tjenester fungerer sikkert, skalerbart og effektivt.

Operational serverinfrastruktur	<i>Operativsystemer og virtualisering:</i> Linux-distributioner som <i>Ubuntu</i>, <i>Red Hat Enterprise Linux</i> og <i>Fedora</i> anvendes bredt. Virtualiseringsværktøjer som <i>KVM</i>, <i>Xen</i>, <i>QEMU</i> og containerteknologier som <i>Docker</i> og <i>containerd</i> muliggør effektiv ressourceudnyttelse. <i>Databaser og dataplatforme:</i> Løsninger som <i>PostgreSQL</i>, <i>MariaDB</i>, <i>Redis</i>, <i>Elasticsearch</i> og <i>Apache Kafka</i> danner grundlaget for databehandling, søgning og realtidsintegration.
Netværk og load balancing	Der findes en række open source-løsninger, som anvendes til skalering og trafikstyring samt sikkerhed, herunder <i>HAProxy</i> , <i>Nginx</i> , <i>Traefik</i> og <i>Envoy</i> .
CI/CD og DevOps-værktøjer	Open source-værktøjer som <i>GitLab</i> , <i>Jenkins</i> , <i>ArgoCD</i> , <i>FluxCD</i> , og <i>Tekton</i> anvendes til Continuous Integration (CI) og Continuous Deployment (CD), dvs. udvikling, test og udrulning af digitale løsninger.

3.2 Udvikling og styring af open source-software

En anden vigtig skelnen inden for open source-software er, hvem der står bag udviklingen, og hvordan styringen – eller governance – er organiseret, da dette har betydning for blandt andet kodekvalitet, opdateringsfrekvens og sikkerhedstjek. Open source-software kræver i de fleste tilfælde en robust governance-model, der skal sikre, at koden vedligeholdes, opdateres og dokumenteres korrekt, hvilket er afgørende for, at open source-projekter er bæredygtige og sikre at anvende over tid. En sådan governancemodel kan fx indebære:

- Regelmæssig gennemgang og vedligeholdelse af koden
- Dokumentation af udviklingshistorik, versionering og sikkerhedsopdateringer
- Transparens om, hvem der står bag projektet, og hvordan beslutninger træffes.

Dette kan sikres på flere forskellige måder. Noget open source-software er bygget af frivillige enkeltpersoner, der bruger deres fritid på at udvikle software. Dog er langt det meste open source-software, der anvendes af offentlige myndigheder i dag, bygget og drevet af virksomheder eller organisationer.

Nogle virksomheder som Red Hat, Meta og IBM udvikler og vedligeholder open source-software som en del af deres forretningsstrategi, da det fx giver mulighed for at præge markedet i en bestemt retning, tilbyde kommerciel support, konsulenttydelser og udvidede versioner af softwaren til betalende kunder. I andre tilfælde går virksomhederne sammen i branchefællesskaber, hvor flere virksomheder samarbejder om at udvikle og vedligeholde open source-software i formaliserede partnerskaber. Her er formålet ofte at deles om udgifterne samt sikre standardisering og interoperabilitet, altså at virksomhedernes kommercielle it-produkter kan fungere sammen.

Organisationer som Apache Software Foundation, Eclipse Foundation, Linux Foundation og Mozilla Foundation er non-profitorganisationer, der blandt andet står bag projekter som Apache HTTP Server,

Kafka, Linux Kernel, Kubernetes og Firefox. De modtager en stor del af deres midler fra store virksomheder som Google, Microsoft, Amazon og Meta, der både bidrager med økonomiske og tekniske ressourcer. Virksomhederne støtter disse organisationer, da det giver dem indflydelse på den teknologiske retning, adgang til stabile og sikre løsninger, og fordi det understøtter deres egne it-økosystemer og produkter. Nedenfor gennemgås fire af de typiske governance-modeller for open source-software. Der findes dog andre modeller, og i praksis kan der også ses kombinationsmodeller mellem fx foundation-drevet software og kommercielle interesser.

Tabel 3. Governance-modeller for open source-software

* Foundation-drevet open source-software Nonprofitorganisationer driver softwaren og sikrer governance, transparens og fællesskabsstyring.	
Kendetegn: Klar governance-model, fællesskabsdrevet udvikling, veldokumenteret og ofte støttet af erhvervslivet	Eksempler: • Apache Software Foundation: Apache HTTP Server, Kafka • Linux Foundation: Linux Kernel, Kubernetes • Mozilla Foundation: Firefox
* Virksomhedsdrevet open source-software Kommercielle virksomheder udvikler og vedligeholder softwaren ofte som en del af deres forretningsstrategi.	
Kendetegn: Styres af en virksomhed, der kombinerer open source med kommercielle interesser, produkter og services	Eksempler: • F5 Inc.: NGINX, webserver med sikkerhedsopdateringer og kommerciel support • Red Hat: Ansible, Fedora
* Konsortium-/branchefællesskabsdrevet open source-software Flere virksomheder samarbejder om at udvikle og vedligeholde software i formaliserede partnerskaber.	
Kendetegn: Fremmer interoperabilitet og standardisering og ofte brugt i infrastrukturprojekter	Eksempler: • Cloud Native Computing Foundation (CNCF): Helm, Prometheus • OpenJS Foundation: Node.js, Electron
* Community-drevet open source-software Softwaren er udviklet af enkeltpersoner eller frivillige fællesskaber uden en større organisation bag.	
Kendetegn: Ofte niche-orienteret, afhængig af frivilligt arbejde, varierende modenhed og governance	Eksempler: • Audacity: Lydredigeringsprogram • Home Assistant: Hjemmeautomationssoftware med fokus på privatliv • Blender: Avanceret 3D-modelleringssoftware, delvist community-finansieret

Det er centralt at forstå de forskellige typer af open source-software og deres governance-modeller for at kunne vurdere den mulige anvendelse blandt offentlige myndigheder. Foundation- og virksomhedsdrevet open source-software tilbyder fx ofte højere sikkerhed og modenhed, mens community-drevet open source kan være en kilde til innovation og nicheløsninger. Governance bør derfor altid være en central overvejelse i valget af open source-software.

3.3 Inbound eller outbound open source-software

Der er en central distinktion mellem, om open source-software anvendes som en aktiv ressource i myndighedernes egen it-udvikling (inbound), eller om myndighederne aktivt bidrager til udviklingen af eksisterende eller nye open source-komponenter, som kan anvendes af andre (outbound). Disse tilgange bør ikke ses som hinandens modsætninger, men som komplementære. Fx kan en stærk inbound-praksis danne grundlaget for en senere outbound-strategi, ligesom outbound-løsninger kan bygge videre på eksisterende open source-løsninger, som er anvendt (inbound).

Tabel 4. Inbound- og outbound-tilgang

 Inbound-tilgang	 Outbound-tilgang
En inbound-tilgang indebærer, at en myndighed enten selv eller via sine leverandører anvender eksisterende open source-software som en del af sin it-portefølje. Her er fokus på at tilpasse, integrere og udnytte allerede udviklet open source-software. Et eksempel er open source-løsningen Apache Kafka, der er så hyppigt anvendt, at det er blevet industristandard for håndtering af datastrømme, dvs. hvordan it-systemer modtager data og sender dem videre. Det anvendes af blandt andet Domstolsstyrelsen (se afsnit 6.3) og en række andre myndigheder, der kan tage løsningen ned fra hyl- den og indarbejde det i deres it-systemer frem for at udvikle den samme funktionalitet på ny.	En outbound-tilgang indebærer, at en myndighed aktivt udvikler og deler open source-software. Formålet er at skabe værdi for både egen organisation og fællesskabet, ved at stille open source-produkter frit til rådighed, så flere kan drage nytte af dem, samtidig med, at myndigheden selv får gavn af andres videreudvikling af produktet. Et andet formål kan være at give offentligheden indsigt i løsningens opbygning. Et eksempel er office- og samarbejdsløsningen openDesk, der er udviklet af den tyske myndighed ZenDiS (se også afsnit 7.1.2). ZenDiS har udviklet openDesk som en open source-løsning, som de stiller til rådighed for alle. Derudover varetager de driften af løsningen for de tyske myndigheder.

3.4 Sikkerhedsaspekter i open source-software

Sikkerhed er en central faktor i vurderingen af open source-software, uanset om myndighederne anvender det inbound eller outbound. Ofte bliver debatten om sikkerheden af open source-software dog sort-hvid. Nogle fremhæver, at open source-software er mere sikkert end proprietær software, da der er mange øjne til at se koden igennem. Andre mener, at da åben kode ikke altid har en tydelig ejer, der opdaterer og vedligeholder den, kan den med tiden udgøre en sårbarhed i myndighedernes it-systemer, da ondsindede aktører kan finde sårbarheder i koden.

Som ovenstående gennemgang af forskellige governance-modeller viser, er der stor forskel på open source-løsninger. Open source-løsninger med stærk governance, som fx foundation- eller virksomheds-drevet open source-software, har ofte etablerede processer for sikkerhedsopdateringer og håndtering af sårbarheder. Omvendt kan noget community-drevet open source-software være umodent eller mangle løbende opdateringer, hvilket gør det mere usikkert at anvende med mindre, at der prioriteres ressourcer og kompetencer hos anvenderen til løbende at vurdere og opgradere koden. Vedligeholdelse er derfor et centralt aspekt i forhold til sikkerhed: selv den mest sikre kode kan blive usikker, hvis den ikke løbende opdateres og testes i takt med nye trusler og teknologiske ændringer.

Sikkerhed i software handler derudover ikke kun om kodekvalitet og sårbarheder – det handler også om, hvordan følsomme elementer som hemmelige algoritmer, certifikater og sikkerhedsnøgler håndteres. Disse elementer kan beskyttes og administreres forsvarligt i både open source- og proprietære løsninger, og valget mellem dem bør derfor baseres på en konkret vurdering af den samlede sikkerhed og risikoprofil, snarere end på kildekodens åbenhed alene.

Det skal desuden understreges, at inbound open source-komponenter sjældent anvendes direkte "ud af boksen". De downloades og implementeres som en del af større systemer, hvor de tilpasses og konfigureres til den specifikke forretningsmæssige kontekst. Det betyder, at sikkerheden ikke alene afhænger af komponentens oprindelige kvalitet, men også af, hvordan den integreres og vedligeholdes i det samlede systemlandskab.

Case: Anvendelse af FreeOTP i staten

Et eksempel på, hvordan inbound open source-software kan understøtte høj sikkerhed, er brugen af komponenten FreeOTP, i mange statslige myndigheders login-system. FreeOTP er en open source-løsning til to-faktor-autentifikation, som anvendes i staten via Statens It og den danske leverandør Semaphore. Selve kildekoden vedligeholdes internationalt af Red Hat. FreeOTP er en central sikkerhedskomponent, der i kraft af sin åbne karakter kan inspiceres og verificeres af uafhængige eksperter.

Omvendt er der situationer, hvor særligt outbound open source-software, altså at myndighederne offentliggør deres kildekode, ikke nødvendigvis er hensigtsmæssigt. Det er fx tilfældet i nogle offentlige apps, hvor der kan ligge en risiko i, at systemets funktionalitet og visuelle brugergrænseflade kopieres én-til-én af uvedkommende. Her kan offentlig adgang til koden potentielt gøre det nemmere at skabe visuelt tro kopier, hvilket kan underminere tilliden til løsningen og øge risikoen for udvikling af apps med falske identiteter. I sådanne tilfælde kan lukkede systemer med stærk kontrol med adgangen til kildekoden være at foretrække.

3.4.1 Sikring mod ondsindede ændringer i open source-software

Når myndighederne vælger at anvende open source-software inbound eller deler egen kode outbound vil de typisk, eventuelt i samarbejde med deres it-leverandører, følge en række sikkerhedsprincipper og -processer, der skal sikre klart ejerskab og ansvar for brug af koden og minimere risikoen for, at personer med skadelige hensigter får deres ændringer ind i koden, som senere kan ende i produktion.

Det indebærer fx, at der er udpeget et team eller en ansvarlig rolle, som har det sidste ord i forhold til, hvilke ændringer der må blive en del af den færdige software. Ingen kan derfor alene bestemme, at ny kode bliver taget i brug. Gennemsigtighed og kontrol af alle ændringer gennemgår en formel proces, hvor de bliver gennemset og godkendt af flere uafhængige personer. Kun ganske få betroede personer har rettigheder til at lægge ændringer ind i den endelige version. Derudover gennemføres typisk automatiske sikkerhedstjek af systemer, der gennemgår al ny kode for fejl og kendte sårbarheder, inden den kan tages i brug. Dette skal sikre, at potentielt skadelig kode opdages og stoppes tidligt i udviklingsprocessen. Tilsvarende vil der som en del af sikkerhedsprocesserne typisk også være en plan for at rulle tilbage til den senest fungerende version af softwaren med det samme og sikre, at skaden bliver minimeret, hvis en ondsindet ændring bliver opdaget.

Samlet handler det om, at myndighederne tager aktivt stilling til kombinationen af ansvar, gennemsigtighed, begrænset adgang, tekniske kontroller og beredskab, inden de beslutter, hvorvidt de ønsker at anvende eller dele open source-software.

3.4.2 Sikkerhedsproblemstillinger ved kritisk infrastruktur

Kritisk infrastruktur handler om systemer og tjenester, der er helt afgørende for samfundets funktion og stabilitet fx energi, vandforsyning, kommunikation, transport og digitale netværk. I disse sammenhænge er spørgsmålet om sikkerhed særligt centralt.

Der er en iboende spænding mellem brugen af open source-software og sikring af kritisk infrastruktur. På den ene side kan open source-software potentielt styrke gennemsigtighed og uafhængighed i kritisk infrastruktur og bidrage med et fællesskab af bidragydere, hvilket kan føre til hurtigere fejlrettelser. På den anden side giver den åbne natur af kildekoden også potentielle angribere en detaljeret vejledning i, hvordan et system er opbygget, og hvor dets svagheder kan ligge. Hvis ondsindede aktører får adgang til detaljerede oplysninger om systemernes arkitektur og implementering, kan de bruge denne viden til at finde sårbarheder og udvikle mere sofistikerede angreb. Risikoen er, at det kan medføre alvorlige skader på samfundets stabilitet og sikkerhed.

Når der arbejdes med systemer af afgørende betydning for samfundets funktion, er det derfor nødvendigt at være særligt forsigtig med at gøre systemerne open source – ud fra et hensyn om at beskytte oplysninger, der kan misbruges af fjendtlige aktører. Der kan således være en generel risiko ved at stille koden bag samfundskritisk software frit tilgængeligt, da det kan udstille eventuelle svagheder over for aktører med negative hensigter. Der er derfor behov for, at myndighederne i endnu højere grad end ved andre typer af it-systemer tager aktivt stilling til, hvorvidt softwaren kan deles, uden at eventuelle sårbarheder kan udnyttes.

Myndigheder, der arbejder med systemer af afgørende betydning for samfundets funktion, skal derudover tage særlige hensyn, såfremt de vælger at anvende open source-software inbound eller deler koden outbound. For at understøtte sikkerheden bør der fx fastlægges klare retningslinjer for, hvordan tekniske oplysninger håndteres i forbindelse med open source-software. Dette kan blandt andet indebære øget fokus på sikkerhed i de interne procedurer for godkendelse af offentliggørelse, styrket informationssikkerhedskultur og en systematisk vurdering af risici ved anvendte open source-software-komponenter.

Det er samtidig nødvendigt at betragte al dokumentation, der viser, hvordan open source-løsninger er implementeret i kritiske systemer, som følsomme oplysninger. Det gælder blandt andet arkitekturtegninger, tekniske implementeringsdetaljer og konfigurationsfiler. Sådanne oplysninger bør klassificeres på passende niveau alt efter systemets samfundsmæssige betydning. Arkitektur, integrationspunkter og konfigurationsdetaljer bør således kun være tilgængelige for betroede parter med et klart behov.

4. Rammer for anvendelse af open source-software

I Danmark er der ikke fastsat centrale regler for, hvornår eller hvordan myndighederne skal anvende eller bidrage til open source-software.

Som en del af statens it-politik lancerede den daværende regering tilbage i 2003 en dansk softwarestrategi, hvor man under princippet ”Bedst og billigst uanset softwaretype” fastslog, at den enkelte myndighed skulle have mulighed for at erhverve den bedste og billigste software ud fra lokale forvaltningsmæssige behov, uanset om der var tale om proprietær eller open source-software.³ I forlængelse heraf blev der gennemført et pilotforsøg med open source-software-kontorpakker hos udvalgte myndigheder. Forsøget viste, at der på daværende tidspunkt ikke var grund til at ændre på princippet ”Bedst og billigst uanset softwaretype”. Det har således været op til hver enkelt organisation at beslutte, om den vil anvende og bidrage til open source-software.

Danmark har dog en tradition for at arbejde med open source-software på udvalgte områder samt med åbne standarder for software i den offentlige sektor.⁴

Open source og åbne standarder



Open source og åbne standarder er beslægtede, men ikke det samme. Open source dækker over software, hvor kildekoden er frit tilgængelig, så andre har mulighed for at tilgå, tilpasse, videreudvikle og videredistribuerer software efter eget behov. Åbne standarder dækker over offentligt tilgængelige tekniske specifikationer, som gør det muligt for forskellige systemer at kommunikere med hinanden uafhængigt af software. Hvor open source fokuserer på selve softwaren, handler åbne standarder om at sikre interoperabilitet gennem fælles regler og formater.

Der er over årene udviklet en række principper, metoder og vejledninger, der kan understøtte myndighedernes anvendelse af open source-software i de tilfælde, hvor det er relevant. Mest centralt står Den Fællesoffentlige Digitale Arkitektur (FDA), der giver en fælles ramme for offentlige it-projekters arbejde med arkitektur. FDA-principperne og de underliggende arkitekturregler indeholder blandt andet anbefalinger om at anvende åbne og internationale standarder, undgå afhængighed af leverandører og proprietære teknologier samt at stille data og løsninger til rådighed for private.⁵ Dertil udstilles et katalog over byggeblokke med henblik på genbrug.⁶

Som led i arbejdet med FDA blev der i 2024 udgivet en vejledning om brug af open source i den offentlige sektor.⁷ Målgruppen for vejledningen er både medarbejdere og strategiske beslutningstagere, der skal tage stilling til it-anskaffelser, og som ønsker mere viden, konkrete eksempler og praktisk vejledning.

På det kommunale og regionale niveau er der også gennemført mange initiativer blandt andet af KL og i sammenslutningerne 4S og OS2 (se mere herom i afsnit 5.2).

³ <https://www.ft.dk/samling/20041/almindeligt/bilag/52/134792/index.htm>

⁴ [Open Source Software Country Intelligence Report - Denmark](#) og [Denmark 2024 - Country Intelligence Report](#)

⁵ [Principper og regler | Fællesoffentlig Digital Arkitektur](#)

⁶ [Digitale byggeblokke | Fællesoffentlig Digital Arkitektur](#)

⁷ [Vejledning om brug af open source i den offentlige sektor | Fællesoffentlig Digital Arkitektur](#)

Case: Aarhus Kommune

Aarhus Kommune har længe haft et fokus på anvendelsen af open source. I 2011 vedtog Aarhus Byråd et krav om, at kommunen overvejer brugen af open source hver gang, at nye it-løsninger anskaffes. I tillæg hertil vedtog kommunen i 2014 en handlingsplan for open source med formålet at øge brugen af open source-software for at undgå leverandørbinding til it-virksomheder.⁸

I 2025 har kommunen vedtaget en digitaliseringsstrategi for 2025-2029, hvor et af målene er at styrke den digitale handlefrihed.⁹ Kommunen har derfor igangsat en række tiltag, herunder foretaget et skifte fra proprietære leverandører til open source-leverandører på udvalgte områder.¹⁰ Derudover blev det i forbindelse med budgetforliget for 2026 besluttet at afsætte 3 mio. kr. årligt i 2026-2029 til at nedbringe udgifterne til it-licenser på kontorpakkeløsninger med henblik på at skabe mere frit valg af leverandører og mere omkostningsbevidst it.¹¹

I dag anvendes open source- og proprietære løsninger side om side i magistratsafdelingerne. Kommunens erfaring er, at det sjældent gavner at anlægge en enten-eller-tilgang, idet det kommunale digitale landskab er nuanceret og kræver fleksible, forretningsdrevne valg.¹² Blandt andet kan hensyn til driftssikkerhed, it-sikkerhed, forretning, styring og bindinger til eksisterende systemer gøre, at proprietære løsninger vælges.¹³

⁸ [Handlingsplan for OpenSource i Aarhus Kommune.pdf](#)

⁹ [Digitaliseringsstrategi](#)

¹⁰ https://pro.ing.dk/digitech/artikel/microsoft-alternativer-og-nye-krav-til-it-leverandorer-saadan-vil-aarhus-kommune-styrke-sin?utm_source=newsletter&utm_medium=email&utm_campaign=digitech

¹¹ [Budget 2026](#)

¹² [Microsoft Word - Svar på 10 dages høringsforespørgsel fra Socialistisk Folkparti - Open Source](#)

¹³ https://pro.ing.dk/digitech/artikel/microsoft-alternativer-og-nye-krav-til-it-leverandorer-saadan-vil-aarhus-kommune-styrke-sin?utm_source=newsletter&utm_medium=email&utm_campaign=digitech

5. Danske myndigheders erfaringer

For at belyse danske myndigheders erfaringer med open source-software er der gennemført en række kvalitative interviews med nøglepersoner fra kommuner, regioner og statslige myndigheder. Dertil er der foretaget interviews med organisationer, der understøtter myndighedernes anvendelse af open source-software (OSPO'er). Der er ikke udarbejdet en kvantitativ analyse af myndighedernes anvendelse, hvorfor analysen primært identificerer tendenser på baggrund af respondenternes erfaringer. Myndighederne er udvalgt med henblik på at sikre repræsentative perspektiver på open source-software, så fx myndigheder med både høj og lav grad af anvendelse af open source er interviewet. Formålet er at forstå, hvordan organisationerne anvender, bidrager og forholder sig til open source-software.

Tabel 5. Interviewoversigt

	Myndigheder der anvender open source-software
Der er gennemført interviews med udvalgte myndigheder med henblik på at sikre både det kommunale, regionale og statslige perspektiv. Derudover er der både valgt større og mindre myndigheder samt myndigheder med varierende fokus på og erfaring med open source-software.	
Kommuner: Favrskov Kommune, Hørsholm Kommune og Odense Kommune	
Regioner: Region Hovedstaden og Region Sjælland	
Styrelser: Erhvervsstyrelsen, Statens It, Sundhedsdatastyrelsen og Udviklings- og Forenklingsstyrelsen	
	Open source-programkontorer (OSPO'er)
Der er gennemført interviews med open source-programkontorer. OSPO'er arbejder for at fremme samarbejdet om open source-software på tværs af aktører, og de støtter deres medlemsorganisationer - i dette tilfælde myndigheder - og bidrager til at skabe et velfungerende og sammenhængende open source-økosystem.	
OSPO'er: 4S og OS2	

5.1 Myndighedernes erfaringer

Det følgende afsnit gennemgår nogle af de erfaringer, som de interviewede myndigheder har gjort sig med open source. Alle myndigheder har erfaring med at anvende open source-software både på desktoplaget og serverlaget.

På desktoplaget har myndighederne erfaring med standardprogrammer som fx Firefox, webapplikationer, desktopsoftware og mobilapps, hvor slutbrugeren ikke mærker, at de anvender et produkt, der er open source-software. Enkelte af myndighederne tilkendegiver, at de eksperimenterer med fx Libre-Office eller lignende open source-tekstbehandlingsprogrammer som et supplement til proprietære softwareløsninger, men ingen har valgt at implementere det på tværs af organisationen. Der er bredt kendskab til mulighederne for at anvende open source på desktoplaget, men enkelte myndigheder beretter, at der på dette område vil være tekniske, organisatoriske og kulturelle udfordringer ved at skifte væk fra de alment kendte tekstbehandlingsprogrammer, som vil skulle overvindes i forbindelse med implementering.

På serverlaget er der større forskellighed, idet myndighedernes tilgang ofte defineres af de it-ansvarlige, der i flere af de interviewede myndigheder har en praktisk tilgang til, hvorvidt der skal anvendes proprietær eller open source-software.

Generelt beretter myndighederne, at de vælger den softwareløsning, som bedst opfylder deres behov, og hvor der samtidig kan indgås en support- og vedligeholdelsesaftale med leverandøren eller med en tredjepart. Yderpolerne mellem myndighederne går fra én myndighed, der anvender open source-software som en strategisk indsats for at mindske udgifterne til software og skabe større selvbestemmelse over deres softwareportefølje, til en anden myndighed, hvis strategi primært er fokuseret på proprietær software, da den ikke har kompetencerne til at håndtere open source-software internt. Flere myndigheder ligger et sted imellem, hvor de anvender open source-software afhængigt af, hvad der vurderes som det umiddelbart bedste valg i den konkrete situation.

Tilsvarende viser de gennemførte interviews, at myndighederne primært anvender foundation-drevet, virksomheds-drevet og konsortium/branchefællesskabs-drevet open source-software. Myndighederne udvikler også egne løsninger, som oftest kan betragtes som in-house software.

Når der kigges ned under motorhjelmene på it-systemerne hos de interviewede myndigheder, vil det aktuelle billede således typisk vise en hybridløsning bestående af både proprietær software, open source-software og egenudviklet kode.

5.1.1 Organisation og implementering

Myndighederne vurderer, at arbejdet med open source-software stiller en række krav til deres organisation. Myndighederne skal have de kompetencer, som det påkræver at tage ansvar for softwarens kvalitet og sikkerhed eller have kompetencerne til at finde eksterne leverandører, der kan varetage opgaven. Myndigheder, der ikke har investeret i open source-kompetencer, beretter, at de stadig er i stand til at anvende open source-software, men i højere grad er afhængige af, at der er en leverandør eller anden ekstern part, der er i stand til at håndtere fx support og vedligeholdelse. Særligt de mindre myndigheder fortæller, at de ikke kan opbygge tilstrækkelige kompetencer og ressourcer, hvis softwaren fx kræver egenudvikling, eller når myndighederne skal indgå i den løbende dialog med et open source-fællesskab.

Flere myndigheder beretter, at der med omstilling til brug af open source-software er behov for høj grad af organisatorisk omstillingsparathed og evne til forandringsledelse. Dette gør sig særligt gældende ved implementering af open source-software på desktoplaget, hvor hver enkelt medarbejder skal uddannes i en ny brugergrænseflade og funktionalitet. Derudover vurderer flere myndigheder, at overgangen til open source-software ofte vil kræve en kulturændring blandt både medarbejdere og ledere, der skal tage ny software i brug og ændre arbejdsgange. Enkelte myndigheder nævner i den forbindelse, at de proprietære softwareløsninger er foran på brugervenlighed og funktionalitet, men at deres oplevelse er, at når først brugerne er blevet oplært i den nye open source-løsning, mindskes modstanden over tid.

I serverlaget er det i begrænset omfang slutbrugeren, der bliver påvirket af implementeringen af open source-software. Myndighederne oplever således lavere grad af organisatorisk modstand på dette niveau. Her er det i høj grad den enkelte it-afdeling, der træffer beslutning om softwareindkøb, særligt af software, der har karakter af redskaber til brug for it-afdelingen. Det skyldes blandt andet, at anvendelsen af open source-software i nogle myndigheder er begrænset til enkelte medarbejdere i it-afdelingerne, som går særligt op i anvendelsen af open source-software. I andre myndigheder er der truffet en aktiv strategisk beslutning om, at open source-software skal udgøre en større andel på tværs af it-porteføljen, hvorfor der ikke er plads til samme autonomi i it-afdelingen.

Eksempler på tilgange til open source-software blandt myndighederne



- * **Aktiv:** Myndigheden har truffet et aktivt tilvalg om, at softwaresammensætningen primært skal være enten proprietær eller open source.
- * **Situationsbestemt:** Myndighedens open source-forvaltning foregår via leverandører, og organisationen deltager ikke direkte i fællesskaber. Anvendelsen sker på baggrund af praktiske behov og er til tider drevet bottom-up frem for af strategiske hensyn.
- * **Ingen strategi:** Myndigheden har ikke taget stilling til anvendelsen af open source-software. Open source-software er dog alligevel en del af myndighedens software, der fx introduceres gennem ad hoc-anvendelse og leverandørernes brug af open source-komponenter i proprietær software.

Myndighederne har meget forskellige erfaringer med rekruttering af de rette kompetencer til open source-området. Én myndighed har udfordringer med at tiltrække medarbejdere med de rigtige kompetencer og kan kun fastholde dem i kort tid, inden de søger videre til andre - enten mere spændende eller bedre betalte stillinger - når først de er oplært. En anden myndighed påpeger, at de på open source-projekter har haft lettere ved at rekruttere medarbejdere med de relevante kompetencer, da deltagelsen i open source-fællesskaber og muligheden for at påvirke retningen for en softwareløsning har givet motivation og arbejdsglæde blandt deres it-udviklere. En tredje myndighed mener, at et aktivt engagement i open source-fællesskabet vil give begrænset værdi, og at det kræver nogle særlige kompetencer, som vil være for dyre at opdyrke internt.

5.1.2 Support og vedligeholdelse

Softwaresupport omhandler assistance til brugere af softwareapplikationer og kan typisk omfatte fejlfinding, træning og teknisk assistance. Der er tale om to typer support afhængigt af, om support henvender sig til slutbrugerne eller teknikerne. I det følgende omtales begge dele samlet, da det vurderes, at erfaringerne med support af open source-software i høj grad er overlappende for de to typer support.

Når der indkøbes open source-software, beretter myndighederne, at der skal træffes aktiv beslutning om, hvordan software-supporten skal håndteres. Det kan foregå internt, hos leverandøren eller ved at indkøbe software-support hos en virksomhed, der specialiserer sig i dette. Når myndighederne vælger at håndtere det internt, skal de ansætte medarbejdere med de relevante kompetencer eller på anden vis opbygge intern kapacitet til at engagere sig i open source-fællesskaber. Flere myndigheder har erfaringer med dette, men kun på konkrete fagområder eller for specifikke softwareløsninger. Når support til open source-software indkøbes i markedet, stilles der større krav til leverandørens modenhed og evne til at håndtere myndighedernes krav, mens det samme gør sig gældende for myndigheder, som vælger at håndtere support internt. Nogle myndigheder ser en værdi i at indgå eksterne supportaftaler med henblik på at minimere interne afhængigheder og have en klar ansvarsfordeling, fx i forbindelse med nedetid og sikkerhedshændelser. En myndighed har gode erfaringer med at anvende strukturerne for support og vedligeholdelse i OS2-samarbejdet, da omkostningerne dermed deles mellem flere myndigheder.

Software vedligeholdelse og videreudvikling er en løbende proces, der indebærer ændringer og opdateringer af software efter den første implementering. Formålet er at imødekomme forskellige behov, herunder fejlrettelser, forbedret ydeevne og tilpasning til ændrede teknologiske eller organisatoriske miljøer. Vedligeholdelse er en afgørende del af softwareudviklingens livscyklus og sikrer, at softwaren forbliver funktionel, pålidelig og i stand til at opfylde skiftende brugerkrav.

Mange af de interviewede myndigheder får softwaren vedligeholdt af deres leverandører. To af de interviewede myndigheder, en kommune og en region, har dog hjemtaget supporten for open source-software på udvalgte forretningsområder og tilpasset denne til deres egne forretningsbehov. Disse

myndigheder står ligeledes selv for driften og vedligeholdelsen af softwaren. Det skyldes, i de nævnte tilfælde, historiske beslutninger, som har vist sig succesfulde, og som i dag understøttes af kontinuitet i kompetencer og ressourcer. Én region bemærker, at de har en stabil drift og råder over interne kompetencer til både drift og vedligeholdelse – en løsning, som de formodentlig ikke ville vælge, hvis beslutningen skulle træffes i dag. Ikke desto mindre fungerer det godt: Systemet kører stabilt, og både support og vedligeholdelse håndteres løbende. Flere myndigheder påpeger ligeledes, at open source-software har den fordel, at det er lettere at fortsætte vedligeholdelse af koden ved at overdrage kilde-koden til en ny ekstern leverandør.

Myndighederne understreger betydningen af robust support og vedligeholdelse som essentielle for succesfuld open source-anvendelse. Konkret beskriver flere myndigheder, at det samme i princippet gør sig gældende for proprietær software. Hvor man ved brug af open source-software er afhængig af et aktivt fællesskab, er man ved proprietær software afhængig af, at leverandøren kan håndtere opgaven - også i det lange løb. Support og vedligeholdelse betragtes generelt som uproblematisk med open source-software, hvis der er etableret samarbejde med eksterne leverandører. Det afgørende er, at der står en moden organisation bag, så koden er forvaltet, aktiv og moden – det vil sige sikker såvel som driftsstabil.

5.1.3 Sikkerhed

Sikkerhed er et vigtigt parameter for myndighederne, når de skal vælge softwareløsning. Det påpeges i flere interviews, at der på sikkerhedsområdet er modsatrettede effekter af den indbyggede åbenhed i open source-software. På den ene side giver det en vis grad af sikkerhed at have adgang til koden og et bredt fællesskab med forskellige kompetencer, der tilgår og retter i koden løbende. Modsat giver dette også ondsindede aktører indsigt i koden og eventuelle sårbarheder.

Myndighederne ser primært sikkerhedsfordele ved open source-software i desktoplaget, hvor flere øjne kan bidrage til hurtigere fejlrettelser og muligheden for at trække på et bredt felt af kompetencer, hvis der er et aktivt fællesskab. Omvendt fortæller flere af de interviewede myndigheder, at de forretningskritisk software i serverlaget i højere grad foretrækker, at koden ikke er offentligt tilgængelig. Generelt påpeger flere myndigheder, at kodens niveau af åbenhed ikke er det vigtigste parameter for sikkerheden. Her gør det sig, ifølge myndighederne, gældende, at sikkerhed primært bygger på robusthed, regelmæssig test og løbende forbedring af koden. Særligt for de typer af open source-software, der ikke har en tydelig ejer, såsom community-baseret open source, er det vigtigt, at myndighederne selv sikrer disse forhold.

Sikkerhedsstandarder

For at højne sikkerhed og transparens vælger mange myndigheder, virksomheder og organisationer at anvende etablerede rammeværk som ISO 27001, der stiller krav til systematisk håndtering og løbende forbedring af informationssikkerheden. ISO 27001 er således valgt som statslig sikkerhedsstandard og har været obligatorisk at følge for statslige institutioner siden januar 2014. Andre arbejder med sikkerhedsinitiativer som Open Secure Software Foundation, hvor strukturerede procedurer understøtter risikohåndtering i open source-projekter.

ISO 27001



- * **Hvad er det?** ISO 27001 er en international standard for informationssikkerhed. Den fastlægger kravene til etablering, implementering, vedligeholdelse og løbende forbedring af et såkaldt Informationssikkerhedsledelsessystem (ISMS). Standarden er teknologineutral og specificerer ikke, om organisationer skal bruge proprietær eller open source-software. I stedet fokuserer den på risikostyring, sikkerhedskontroller og løbende forbedring af informationssikkerheden – uanset softwaretype.
- * **Formål:** At sikre fortrolighed, integritet og tilgængelighed af informationer gennem systematiske sikkerhedsforanstaltninger og risikostyring
- * **Relevans for open source-software:** Myndigheder og virksomheder, der anvender open source-software, bruger ofte ISO 27001 som ramme for at sikre, at open source-løsninger lever op til samme krav om sikkerhed som proprietære systemer

Open Secure Software Foundation (OpenSSF)



- * **Hvad er det?** OpenSSF er et globalt initiativ, der arbejder for at styrke sikkerheden i open source-software. Organisationen blev etableret under Linux Foundation og samler eksperter fra både private virksomheder og offentlige myndigheder
- * **Formål:** At udvikle værktøjer, standarder og bedste praksis, som forbedrer sikkerheden i open source-software-projekter
- * **Relevans for open source-software:** Virksomheder, der anvender open source-software, benytter i stigende grad OpenSSF's værktøjer og anbefalinger til at vurdere og styrke sikkerheden i de open source-komponenter, de benytter.

Når myndighederne er i tvivl om open source-softwarens modenhed og sikkerhedsniveau, er der ofte behov for ekstern bistand. Én myndighed, der anvender open source-software til rolleadministration, indhentede således kompetencer hos en tredjepart til at give programmet et eksternt kode-review. En anden myndighed supplerer, at noget open source-software kræver løbende opdatering og sikkerhedsverifikationer, hvilket kan være en tung administrativ byrde. Hertil beretter en myndighed, at de ikke oplever, at adgang til kildekoden nødvendigvis giver en fordel i forhold til selv at kunne foretage fejlrettelser. Det skyldes, at de ikke selv har de rette kompetencer og således er afhængige af eksterne – enten i et open source-fællesskab eller en leverandør af proprietær software.

Mindre myndigheder er i høj grad afhængige af, at eksterne leverandører står for fx kode-review og disaster recovery-tests. Én myndighed påpeger dog, at ansvaret for sikkerheden i sidste ende altid ligger hos den offentlige myndighed, hvorfor det kun er muligt at udlicitere sikkerhedsopgaven til en vis grad. Modsat påpeger en anden myndighed, at de har behov for, at en ekstern leverandør tager ansvaret på sikkerhedsområdet, så der er en ekstern ansvarlig i forbindelse med fx nedbrud.

5.1.4 Licensstyring og anskaffelse

Helt centralt i definitionen af open source-software står de licenser, der bestemmer anvendelsen af softwaren. Disse licenser kan indeholde forskellige vilkår, fx at brugeren er forpligtet til at dele koden, hvis man videredistribuerer softwaren, eller at programmet ikke må benyttes i kommercielle sammenhænge til fx distribution. Det betyder, at myndighederne potentielt skal forholde sig til nogle andre licensvilkår, end når de indgår kontrakt med en kommerciel leverandør.

Flere myndigheder påpeger, at licensstyring i forbindelse med open source-software er vigtigt, men ikke en væsentlig barriere for anvendelse af open source-software, så længe der ikke sker distribution. Én mindre myndighed vurderer, at open source-software generelt er vanskeligt at håndtere juridisk, hvorfor den er afhængig af ekstern bistand. En anden myndighed har stort fokus på at anvende kendte og klare licenser med kontraktuelle sikkerhedsgarantier fra leverandøren, hvilket letter juridisk håndtering fx ved sikkerhedshændelser.

Anskaffelse indebærer en række procestrin fra den indledende behovsafklaring til evaluering af key performance-indikatorer efter, at softwaren er implementeret for således at sikre, at den lever op til myndighedens behov. En myndighed beskriver, at der i forbindelse med anskaffelse kan være en tendens til, at myndighederne primært afsøger proprietære løsninger. Samtidig påpeger myndigheden, at processen i den ideelle verden burde være helt åben, og valget af enten proprietær eller open source-software dermed burde afhænge af, hvilken software der bedst kan imødekomme det behov, som myndigheden har defineret i starten af anskaffelsesprocessen. Dette kan dog være svært at leve op til i praksis.

En myndighed oplever, at man med bestemte open source-software-programmer kan mindske leverandørafhængighed, fx ved anvendelse af database-software som MySQL, som flere forskellige leverandører har de rette kompetencer indenfor. En anden myndighed oplever, at selvom open source-software kan bidrage til leverandøruafhængig, kan overgangen til open source-software i nogle tilfælde kræver en så stor investering, at muligheden kan virke mere teoretisk end realistisk.

5.1.5 Integration til anden software

Offentlige myndigheder navigerer i et meget omfattende it-systemlandskab. Ifølge Finansministeriets Budgetredegørelse for udgiftspolitik styring af it-området fra 2023 er der alene på tværs af statens område mere end 2.700 it-systemer. Det er derfor essentielt, at ny software kan integreres med myndighedernes eksisterende software.

De interviewede myndigheder vurderer generelt, at open source-software ikke skaber selvstændige integrationsproblemer, da det typisk følger åbne standarder og moderne API'er. Ved overgangen til open source-software har flere myndigheder dog oplevet udfordringer med den tilbageværende proprietære software. Nogle myndigheder påpeger også, at open source-software er lettere at integrere med eksisterende software, da proprietær software til tider kræver, at kunderne holder sig til en bestemt softwaretype. Samtidig har flere myndigheder investeret i at opbygge integrationer mellem proprietær software og fx ESDH-systemer, hvorfor det kan være en omfattende proces at erstatte de eksisterende softwareløsninger med open source-software.

5.1.6 Økonomi

Størstedelen af de adspurgte myndigheder har ikke en egentlig strategi for, hvorvidt de ønsker at bruge open source-software. En myndighed beskriver, at valget falder på open source-software, når det giver både økonomiske og funktionelle fordele. En anden anbefaler, at man udarbejder en total cost of ownership-analyse, da open source-software ofte er gratis at anskaffe, men vil kræve vedligeholdelse

og support samt et aktivt engagement i softwarens fællesskab. Derfor påpeger myndigheden, at det er særligt vigtigt at estimere software ud fra de samlede levetidsomkostninger frem for på indkøbsprisen eller licensbesparelser i sig selv. Open source-software har således en anderledes omkostningsprofil end proprietær software.

Kompetencespørgsmålet har også en betydning for de økonomiske overvejelser, som myndighederne gør sig. En myndighed påpeger, at når der ikke er en leveringspligtig organisation bag softwaren, stiller det krav til, at organisationen har midler at investere i udvikling af egen bemanning og kompetencer. Det er særligt udfordrende, når organisationen samtidig skal investere i et setup, der kan facilitere blandt andet leverandørstyring og udbud vedrørende proprietær software og dermed skal have to sideordnede organisationer til at håndtere de to forskellige softwaretyper.

Derudover er der blandede erfaringer med økonomien bag brugen af open source-software. En myndighed vurderer, at besparelsen ikke er ret stor, når den har egenudviklet open source-komponenter, mens den har oplevet en besparelse gennem et forsøg med anvendelsen af LibreOffice som erstatning for Microsoft Office i desktoplaget. Dog har myndigheden i forsøget fastholdt Microsoft Office til mere avancerede funktioner. Enkelte myndigheder har taget alternative kontorpakker i brug i begrænset omfang, da de kan se et besparelspotentiale på licenserne, men der er ikke stor efterspørgsel ved slutbrugerne på at gå væk fra Microsoft Office.

Deling af open source-komponenter kan også have en økonomisk dimension. En af myndighederne påpeger, at komponenten skal have en vis størrelse, før det kan betale sig for myndigheden at afsøge markedet for eksisterende løsninger eller dele løsninger med andre myndigheder frem for at egenudvikle. I den pågældende myndigheds eksempel var der tale om en datokomponent, der ikke kunne betale sig at anvende. Det skyldtes, at det overhead, der skulle til for at integrere den ind i en ny sammenhæng, var så stort, at myndigheden valgte at udvikle den fra bunden.

Flere myndigheder har en forhåbning om, at brugen af open source-software kan bidrage til et mere konkurrenceudsat marked, hvor de i højere grad vil være i stand til at presse priserne på licenser. Det er dog kun én myndighed, der beretter, at open source er med til at skabe et mere dynamisk marked – i dette tilfælde for enterprisedatabaser – hvor der ifølge myndigheden tidligere havde været næsten monopollignende tilstande. Samme myndighed beretter dog, at leverandørafhængigheden afhænger af fagområdet. I forlængelse af dette beretter en kommune, at de tilbyder to forskellige softwarepakker til kommunens medarbejdere. Den ene er fuldt ud baseret på en standard Microsoft-pakke, mens den anden pakke består af så meget open source-software, som det har været muligt for it-afdelingen at inkorporere, hvilket har gjort den billigere end standardpakken. På den måde er det op til den enkelte forvaltning at beslutte, hvorvidt de ønsker at spare penge på licenser – fx til medarbejdere, der i løbet af deres arbejdsdag anvender computere i et mindre omfang og derfor ikke har brug for alle funktionerne i Microsoft Office.

5.2 Danske OSPO'er: OS2 og 4S

I Danmark er der to særligt relevante eksempler på etableringen af open source-programkontorer (OSPO'er, jf. boks nedenfor) i den offentlige sektor: OS2 og 4S. OS2 er en aktiv OSPO forankret i et samarbejde, som primært er kommunalt, med fokus på praktisk anvendelse, leverandøruafhængighed og bæredygtig governance. Den bygger på medlemsfinansiering, fællesskabsudvikling og åbenhed i såvel proces som understøtter praktisk anvendelse af open source i kommunerne.

Senere case-beskrivelse præsenteres OS2 med konkret eksempel på, hvordan open source-software kan organiseres og forankres i den offentlige sektor – på tværs af myndigheder.

Omvendt repræsenterer 4S et mere centraliseret og topstyret initiativ med særligt fokus på sundhedssektoren, herunder kvalitetssikring og regulatorisk compliance. Trods sin tekniske ambition og strukturelle grundighed er arbejdet med 4S pt. sat i bero, blandt andet grundet manglende politisk opbakning og finansiell bæredygtighed.

Hvor OS2 i dag fungerer med en adaptiv og decentral model, fremstår 4S som et eksempel på, at teknisk kvalitet og governance alene ikke kan bære en OSPO – det kræver også bred organisatorisk og økonomisk forankring.

Open Source Program Office (OSPO)



Et OSPO er et kompetencecenter, der styrer, udvikler og optimerer en eller flere organisationers arbejde med open source-software. OSPO'et fungerer som det centrale omdrejningspunkt for arbejdet med open source – både teknisk, juridisk og organisatorisk.¹⁴ Et OSPO har typisk en række ansvarsområder og bidrager til anvendelsen af open source-software på forskellig vis som listet nedenfor.¹⁵

* Hvilke ansvarsområder har et OSPO?

- **Strategi og politikker:** Udformer og implementerer strategier for brug, udvikling og deling af open source-software, herunder retningslinjer for licensering, compliance og sikkerhed
- **Juridisk compliance:** Sikrer overholdelse af licenser og håndtering af juridiske risici forbundet med brug og distribution af open source
- **Uddannelse:** Træner medarbejdere i best practices for anvendelse af open source
- **Kultur:** Fremmer en samarbejdsorienteret open source-kultur på tværs af organisationen
- **Community engagement:** Bygger relationer til open source-fællesskaber og sikrer, at organisationen både bidrager til og drager fordel af eksterne projekter
- **Support og vedligeholdelse:** Understøtter vedligeholdelse af interne og eksterne open source-projekter og repositories¹⁶
- **Forretningsudvikling:** Undersøger og udvikler forretningsmodeller relateret til open source-software.

5.2.1 Support og vedligehold

OS2 sikrer support og vedligehold gennem en governance-model, hvor brugere forpligter sig økonomisk ved tilslutning til et open source-projekt. Anvendelse kræver medfinansiering til både drift og videreudvikling. Support kan købes hos forskellige leverandører, men der stilles krav om gennemsigtighed og mulighed for at skifte leverandør. En udfordring er, at kontrakter ofte involverer flere parter, hvilket kræver, at OS2's medlemmer har kompetencer til at vurdere softwaremodenhed og leverandørmarkedet.

4S lægger vægt på formaliseret support og vedligehold, hvilket de vurderer som særligt vigtigt for sundhedssoftware. Her skal der være bestemte procedurer og kvalitetsstandarder på plads blandt andet for at overholde den gældende regulering på sundhedsområdet.

¹⁴ [Definition of Open-Source Program Office \(OSPO\) - Gartner Information Technology Glossary](#)

¹⁵ [What is an Open Source Program Office and why you should have one - Open Source Initiative](#)

¹⁶ Et repository er et digitalt arkiv, hvor filer og kildekode gemmes, organiseres og versionstyres. Det muliggør samarbejde, deling og sporing af ændringer.

5.2.2 Sikkerhed og licensstyring

Begge OSPO'er ser sikkerhed som afhængig af governance og kildekodens modenhed. Modne open source-projekter håndterer sikkerhedshuller effektivt via åbne processer og dedikerede sikkerhedsteams. OS2 har eksperimenteret med scanning af kildekode og andre sikkerhedstiltag, hvilket de arbejder mod på sigt at tilbyde for alle deres produkter. Tilsvarende vurderer OS2, at licensstyring er vigtigt – især i forhold til copyleft-licenser, hvor ændringer skal deles tilbage med fællesskabet. De har derfor behov for juridiske kompetencer for at sikre licenscompliance.

4S håndterer sikkerhed og licenser ud fra sundhedsreguleringerne. De har udviklet faste procedurer og klare ansvarsfordelinger omkring kildekode og dokumentation. Licenser bliver valgt pragmatisk, men 4S anbefalede som udgangspunkt copyleft-licenser.

5.2.3 Integration til anden software

Begge organisationer vurderer, at open source ikke er sværere at integrere end proprietær software. Adgang til kildekode og dokumentation kan fra deres perspektiv i nogle tilfælde gøre integration enklere, hvis de rette tekniske kompetencer er til stede. Problemer opstår primært, hvis der ikke er anvendt åbne standarder fra start. Begge organisationer fremhæver, at integration med eksisterende systemer lettes, hvis man følger fælles åbne snitflader.

5.2.4 Økonomi

Open source-software i OS2-fællesskabet er gratis at hente og frit tilgængelig for alle offentlige aktører. Det er vigtigt at fremhæve, at softwaren har omkostninger, for løsningerne skal udvikles, tilpasses og vedligeholdes professionelt, og det kræver ressourcer i form af både økonomi og kompetencer.

OS2 arbejder derfor målrettet for at sikre en ansvarlig og bæredygtig model, hvor brugerne bidrager økonomisk – typisk via medlemskab. I OS2 er det et grundlæggende princip, at brug forpligter – og at det fælles ansvar for finansiering er en forudsætning for stabile og effektive løsninger til gavn for den offentlige sektor.

6. Tre danske cases

For at give et mere detaljeret indblik i, hvordan open source-software anvendes blandt offentlige myndigheder i Danmark, er der udvalgt tre illustrative cases.

Den første case er sundhedsvæsenets Nationale Serviceplatform. Den viser, hvordan open source-software anvendes inbound af en dansk offentlig myndighed til at bygge samfundskritisk infrastruktur. Den anden case er OS2-samarbejdet, der viser, hvordan offentlige myndigheder kan gå sammen om fælles udvikling af open source-software. Den tredje case er Domstolsstyrelsens straffe- og skifteprogram. Den viser, at selv når en offentlig myndighed udvikler software, som de selv ejer, kan det være vanskeligt at dele denne software med andre offentlige myndigheder med henblik på genbrug. De tre cases gennemgås nedenfor.

6.1 Sundhedsvæsenets Nationale Serviceplatform

Den nationale serviceplatform (NSP) er en kritisk del af Danmarks digitale infrastruktur inden for sundhedsområdet. Platformen opstod som en løsning på behovet for en centraliseret, robust og skalerbar infrastruktur, der kunne understøtte nationale sundhedssystemer, herunder forretningsservices som fx det Fælles Medicinkort, det Danske Vaccinationsregister med flere samt en række registre såsom Organdonationsregisteret.

6.1.1 Behov for stabilitet og driftssikkerhed

Sundhedsvæsenets parter (regionerne, lægepraksis og kommunernes omsorgssystemer) er afhængige af komponenter og services, som indgår i NSP-infrastrukturen. Derfor har det høj prioritet at sikre driftsmæssig kontinuitet. Infrastrukturens komponenter udformes således med henblik på maksimal driftsstabilitet, tilgængelighed og robusthed, og opgraderinger foretages i mindst mulige skridt for at minimere konsekvenserne af eventuelle problemer.

Et centralt princip bag NSP er ønsket om uafhængighed af specifikke leverandører for at sikre kontinuitet og fleksibilitet i drift og vedligeholdelse. Denne uafhængighed har de blandt andet forsøgt at opnå ved at anvende open source-software.

6.1.2 Valg af egenudviklet og open source-software

Udviklingen af NSP er præget af både egenudviklet software og anvendelse af open source-software. Dette valg er truffet ud fra både strategiske og økonomiske hensyn. De strategiske hensyn er blandt andet et ønske om, at der skal være mulighed for både interne og eksterne kode-reviews. Brugen af open source-software gør det samtidigt muligt at reducere licensomkostninger, især i en distribueret infrastruktur som NSP. Platformens arkitektur bygger på eksisterende open source-systemsoftware-komponenter.

NSP's strategi indebærer desuden anvendelse af en permissive licensform (MIT-licensen), som sikrer en bred og ubegrænset anvendelse af platformens komponenter uden krav om tilbagelevering af ændringer fra brugernes side. Dette åbner op for eksterne leverandører, som dermed har mulighed for at anvende og bidrage til softwaren, hvilket på sigt styrker systemets robusthed og kvalitet.

Et yderligere vigtigt element ved NSP er brugen af åbne internationale standarder, som platformen følger konsekvent. Standardiseringen sikrer bedre kommunikation mellem forskellige systemer og muliggør samtidig en effektiv integration af nye komponenter og services, hvilket reducerer risikoen for tekniske udfordringer.

6.1.3 Kvalitetssikring og driftssupport

Kvalitetssikring og driftssupport for NSP er uddelegeret til specialiserede leverandører, hvilket gør det muligt at opretholde et højt kompetenceniveau, der løbende overvåger og sikrer systemets kvalitet og ydeevne. Dette understøttes af en praksis med regelmæssige kode-review-processer og aktiv opfølgning på brugerfeedback og fejlrapporter.

6.2 OS2 - Et fællesoffentligt samarbejde om digital udvikling

OS2 er et fælleskommunalt samarbejde, der blev grundlagt med det formål at udvikle og dele digitale løsninger mellem danske kommuner og offentlige institutioner gennem åben kildekode og fælles løsninger. OS2 står for "Offentligt Samarbejde og Open Source". Samarbejdet bygger på en filosofi om deling, åbenhed og fælles udvikling, hvor kommuner ikke blot er brugere, men også medskaber digitale redskaber til den offentlige sektor. Tanken er, at løsninger som er skabt eller købt i en kommune, ofte også er relevante for de 97 andre kommuner og at det derfor kan give værdi at udvikle og drive dem i fællesskab.

OS2 har særligt haft gennemslagskraft på det kommunale område både i form af antallet af medlemmer, men også i antallet og udbredelsen af de digitale løsninger. OS2 har i dag en portefølje på 26 it-produkter.¹⁷ Organisationen fungerer som en paraply, hvorunder der kan etableres forskellige projekter og netværk, og hvor det enkelte medlem kan byde ind på eller initiere nye løsninger, som kan deles med andre.

6.2.1 Governancemodel: Fælles styring med lokalt ejerskab

OS2's governancemodel bygger på et fælles sekretariat og en styregruppe, hvor medlemmerne har afgørende indflydelse. Governancemodellen muliggør decentral udvikling inden for rammerne af fælles standarder og principper. Hver OS2-løsning har sin egen projektorganisering, typisk med en styregruppe, produktejer og en bred brugergruppe, som sikrer både strategisk og operationel forankring.

Det betyder, at beslutningskompetencen for den enkelte løsning ligger hos de deltagende medlemmer, hvilket sikrer relevans og ejerskab. Sekretariatet understøtter processer og sikrer koordinering på tværs – herunder at fælles principper, regler og retningslinjer overholdes, men det er fællesskabet, der definerer retningen.

En central funktion for OS2 som OSPO er at tilbyde kvalificeret ekspertbistand til sine medlemmer. Dette sker gennem sekretariatet og projektorganisationerne, som bistår med teknisk rådgivning, juridiske afklaringer (fx licensspørgsmål), leverandørstyring og støtte til udbuds- og implementeringsprocesser. Denne ekspertise kan være vanskelig at opbygge internt, især blandt mindre offentlige myndigheder med begrænsede ressourcer og kapacitet inden for digital udvikling. Derfor kan OS2 som OSPO fungere som en udvidet kapacitet og et videnscenter, som medlemmerne kan trække på, når

¹⁷ <https://www.os2.eu/os2-it-loesninger>

de ønsker at tage del i eller igangsætte open source-projekter. Samtidig understøtter OS2 en kultur for fælles læring og kompetenceudvikling via netværk, workshops og deling af best practices.

6.2.2 OS2-produkteksempler – OS2valghalla og OS2kitos

Et eksempel på en open source-komponent, der er udviklet i regi af OS2, er OS2valghalla. Komponenten understøtter valgafvikling ved at levere et samlet system til rekruttering og håndtering af bemanding i forbindelse med valg. Systemet er bygget op omkring en central forretningskerne, som er blevet udarbejdet gennem workshops, hvor de deltagende kommuner har identificeret fælles forretningsfunktionalitet. Kommuner med behov for yderligere funktionalitet har mulighed for at udvikle ekstra moduler, som også forvaltes af OS2 og deles åbent med øvrige interessenter. OS2valghalla anvendes i dag af 28 kommuner.

Et andet eksempel er OS2kitos (Kommunernes IT-OverblikSystem). Det er en webbaseret løsning, som bruges af danske kommuner til at skabe overblik over deres it-systemer, kontrakter, snitflader, projekter, GDPR-compliance og arkiveringspligt. Systemet giver mulighed for at registrere og vedligeholde information om egne systemer og tilhørende kontrakter, kommunens snitflader, rollefordeling mv. Derudover er der mulighed for lokal tilpasning og konfiguration, idet den enkelte kommune kan tilpasse visningen og styre hvilke moduler, der indføres hvornår. Systemet fungerer desuden i kombination med andre systemer og myndigheder fx ved integration med Det fælleskommunale Databehandlersekretariatet (DBS), hvilket reducerer behovet for dobbeltregistrering. OS2kitos anvendes i dag af 80 kommuner.

6.3 Domstolsstyrelsens straffe- og skifteprogram

Straffe- og skifteprogrammet er domstolenes hidtil største digitaliseringsprogram. Formålet med programmet er at udvikle en ny løsning til at understøtte straffe- og skifteområderne, og programmet blev igangsat i 2020 og forventes afsluttet ved udgangen af 2026.¹⁸

6.3.1 Udvikling af den nye løsning

Programmet gennemføres som et agilt projekt, hvor eksterne udviklere i samarbejde med styrelsens egne medarbejdere udvikler systemet til en ny drifts- og udviklingsplatform. Al udvikling gennemføres på Domstolsstyrelsens adresse.

Udviklingen af de nye systemer tager afsæt i en modulær tænkning, hvor den samlede udvikling sker i en række agile releases gennem en række konkrete og samspillende moduler, hvor der både anvendes tekniske specialist-kompetencer og sagskompetencer. Der gennemføres hyppige demoer og dialog med slutbrugerne med henblik på at sikre, at udviklingen understøtter forrettningens behov.

6.3.2 Mulighed for genbrug af kode og moduler

Mange af de moduler, Domstolsstyrelsen bygger, er moduler, som potentielt kan anvendes flere steder i den offentlige sektor, hvor der er behov for samme type funktionalitet. Det er fx sagsoverblik, integrationer til andre myndigheders oplysninger, generering af PDF-dokumenter, som sendes til borgere og virksomheder via Digital Post, eller det omfattende designbibliotek, programmet har udviklet.

Når straffe- og skifteprogrammet er afsluttet, ser Domstolsstyrelsen en mulighed for, at andre offentlige myndigheder potentielt kan anvende de udviklede moduler. Styrelsen har været i dialog med Kammeradvokaten, som ikke ser noget til hinder for, at kode og moduler genbruges på tværs af offentlige

¹⁸ [Danmarks Domstole - Straffe- og skifteprogrammet](#)

myndigheder, særligt fordi koden er ejet af Domstolsstyrelsen. Ud over den konkrete kode ser Domstolsstyrelsen også et potentiale i at genbruge metoder, rollekataloger med flere, som er grundlaget for systemets 'logik'.

6.3.3 Forudsætninger for genbrug

Domstolsstyrelsen peger på, at der i dag ikke findes ét samlet sted, hvor de kan aflevere deres kode med henblik på genbrug. Foruden et fælles sted til at aflevere sin kode, er der også en række øvrige forudsætninger, som skal være opfyldt for, at deling af kode ikke bliver for stor en opgave – og samtidig sikrer, at koden let kan genanvendes. Følgende spørgsmål fremhæver centrale overvejelser i forhold til disse nødvendige forudsætninger:

- Hvem kan agere mellemlid mellem forskellige myndigheder – deres it-systemer og behov samt med hvilke rammer?
- Skal koden kun kunne genbruges af andre offentlige myndigheder eller også af private interessenter?
- Hvem skal sikre, at koden vedligeholdes, eller skal det tydeligt fremgå, at det er op til anvenderen selv at sikre aktualitet og opdatering ved eventuel ibrugtagning?

Arbejdet med straffe- og skifteprogrammet viser, at open source ikke nødvendigvis er den eneste vej frem, hvis målet er at sikre øget genbrug af it-løsninger i den offentlige sektor og mindre afhængighed af it-leverandører. Casen illustrerer dog også, at det kan være vanskeligt at dele – også selvom potentialet virker indlysende. Den peger derfor på behovet for støtte til myndighederne både i at bygge til genbrug, men også til screening af eksisterende offentlige it-løsninger i forbindelse med nyudvikling.

7. Internationale erfaringer

Dette kapitel giver et indblik i udvalgte landes erfaringer med open source-software samt overblik over væsentlige tiltag inden for open source-software i internationalt regi, herunder EU og FN.

7.1 Erfaringer fra andre lande

Danmark er et af de mest digitaliserede lande i verden, og den danske offentlige sektor har været førende inden for digitalisering i mange år. Det betyder også, at erfaringer fra andre lande, der i mindre grad har digitale offentlige forvaltninger eller fx er underlagt væsentligt anderledes love og regler, ikke altid er direkte sammenlignelige med eller kan overføres til en dansk kontekst. Dog kan andre landes erfaringer med open source-software bidrage med vigtige indsigter og inspiration.

Kortlægning af tilgangen til open source-software

Rapporten "Software Reuse through Open Source-Software in the Public Sector – A qualitative survey on Policy and Practice" fra 2024 er en kortlægning af tilgangen til open source-software i 15 digitalt modne lande.¹⁹ Rapporten viser, at alle landene beskæftiger sig med open source, men at landenes ambitionsniveau, policy og styring af open source-software varierer. Grundlæggende kan landenes tilgange til open source opdeles i tre grupper:

1. **Overordnet strategisk niveau:** I denne gruppe er open source-policy på et overordnet strategisk regeringsniveau. Heri indgår blandt andre Finland og Luxembourg, hvor open source adresseres i landenes regeringsgrundlag, men endnu ikke har udmøntet sig i konkret policy. Der foreligger således en politisk ambition om at arbejde med open source, som endnu ikke er fulgt op med konkret policy eller implementering på området.
2. **Konkret policy-niveau:** I denne gruppe findes lande med konkret policy på open source-området. Heri indgår Danmark og Island, hvor der i begge lande gives retningslinjer for, hvordan open source kan og bør indtænkes på lige fod med andre digitale løsninger.
3. **Operationelt anvendelsesniveau:** I denne gruppe foretrækkes open source eksplicit og anvendes som udgangspunkt, medmindre særlige – fx sikkerhedsmæssige – hensyn gør sig gældende. I Storbritannien gælder dette både for inbound og outbound, mens det i Frankrig, Nederlandene, Spanien (hvor det er lovfæstet) og Estland (hvor myndigheder opfordres til at anvende open source) primært er på outbound-siden, at der er krav eller forventninger om at anvende open source-principper.



Flere digitalt modne lande har indført politiske tiltag på open source-området. Tiltagene kan enten være målrettet anvendelsen af open source-software i den offentlige sektor eller være målrettet anvendelsen i den private sektor, fx gennem industripolitik, uddannelsespolitik eller støtte til open source-fællesskaber. Generelt set er fokus i europæiske og amerikanske regeringspolitikker på den offentlige sektor, mens regeringer i Asien har en tendens til at fokusere på den private sektor.²⁰

I en rapport udarbejdet for EU-Kommissionen fra 2022 konkluderes det, at open source-tiltag rettet mod den offentlige sektor i de undersøgte lande sjældent har været succesfulde²¹. De lande, der

¹⁹ Forskningsrapport

²⁰ [Study about the impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy | Shaping Europe's digital future](#)

²¹ [Study about the impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy | Shaping Europe's digital future](#)

havde indført lovgivning med krav om udvikling og genbrug af open source-software i den offentlige sektor, oplevede ofte, at indsatsen ikke lykkedes – primært på grund af manglende konkret implementeringsvejledning. De mest overbevisende implementeringer fandt sted, hvor open source-software var blevet en kernekomponent i et digitalt skifte og dermed forankret i administrationens digitale kultur.

Nedenfor gennemgås konkrete erfaringer fra udvalgte lande. Landene er udvalgt, da de for det første har gjort sig erfaringer med anvendelsen af open source-software i offentlige myndigheder. For det andet er de udvalgt, da de alle, på nær Schweiz, er EU-medlemslande og dermed har lignende lovgivningsmæssige rammer som Danmark, fx i form af udbudslovgivning og GDPR. Endeligt er landene udvalgt for at vise spændvidden i tilgangen til open source-software i den offentlige sektor internationalt set.

7.1.1 Italien

Italien har siden 2012 haft en lovgivning, der forpligter offentlige myndigheder til som udgangspunkt at vælge open source-software og sikre, at offentligt finansieret software gøres frit tilgængelig. I praksis havde lovgivningen dog begrænset effekt i de første år. Det var først efter, at der fra politisk hold blev nedsat enheder, som fungerede som de facto Open Source Programme Offices (OSPO'er), samt at der i 2019 blev udgivet konkrete retningslinjer for indkøb af open source-software, at lovgivningen for alvor fik effekt.²² Team Digitale blev oprettet i 2016 og fik til opgave at udvikle et slags "operativ-system" for staten – en række grundlæggende digitale komponenter, som andre myndigheder kunne genbruge og integrere i deres egne systemer som led i deres digitale transformation. Team Digitale spillede en nøglerolle i at skabe genbrugelige løsninger og yde rådgivning om både udvikling og indkøb af open source-software i det offentlige. I dag er Team Digitales opgaver forankret i en digitaliseringsafdeling under regeringen, og det er enheden Developers Italia, der som de facto OSPO udgør Italiens centrale platform og fællesskab for offentlig open source-udvikling.

Udviklingen hænger tæt sammen med de treårige nationale strategier for digital transformation, som Italien har arbejdet med siden 2017. Den aktuelle plan for 2024–2026 lægger vægt på open source som et middel til at fremme gennemsigtighed, effektivitet og genbrug på tværs af den offentlige sektor. Planen opstiller ligeledes konkrete målsætninger, herunder at mindst 150 myndigheder skal udgive open source-løsninger via Developers Italia, og at mindst 3.000 offentlige enheder skal genbruge software herfra inden udgangen af 2026.²³ Derudover vil regeringens digitaliseringsafdeling udarbejde et vejledningsdokument om offentlig udvikling og forvaltning af software i overensstemmelse med open source-principper. Desuden er en væsentlig del af Italiens treårsplan udgjort af tiltag dedikeret til open source, der skal forbedre effektiviteten og gennemsigtigheden i den italienske offentlige forvaltning og modvirke leverandør-afhængighed.²⁴

7.1.2 Tyskland

Tyskland har i de senere år løftet open source-arbejdet til føderalt niveau som led i en bredere digital strategi, hvor digital suverænitet spiller en central rolle. Tidligere var indsatser på open source-området primært drevet af lokale initiativer, men med regeringskoalitionen fra 2021 blev der sat en ny retning med en samlet national tilgang. Et vigtigt resultat af denne udvikling var etableringen af ZenDiS i 2022, et aktieselskab ejet af den føderale regering, som udgør et center for digital suverænitet i

²² [Report: Public Sector Open Source Program Offices - Archetypes for how to Grow \(Common\) Institutional Capabilities - Virtual Home of Johan Linåker](#)

²³ [Italy 2025 - Country Intelligence Report\(1\).docx](#)

²⁴ [Italy's public service digital strategy updated | Interoperable Europe Portal](#)

Tysklands offentlige administration.²⁵ Som kompetence- og servicecenter bistår ZenDiS den offentlige administration på føderalt, statsligt og lokalt niveau med at styrke sin langsigtede digitale handlekraft – med særligt fokus på at nedbringe kritiske afhængigheder af individuelle teknologiudbydere. Centret skal blandt andet understøtte det tyske forsvar i at opnå større uafhængighed gennem open source-løsningerne, openDesk og openCode, der skal fungere henholdsvis som office- og samarbejdssuite samt central infrastrukturkomponent.²⁶

Derudover har Tyskland etableret og finansierer den administrative enhed Sovereign Tech Agency, som via en støttepulje understøtter udvalgte decentrale open source-initiativer.²⁷ Sovereign Tech Agency har også et fellowship-program, hvor de i en tidsbegrænset periode aflønner open source-eksperter for deres arbejde med at vedligeholde open source-løsninger. Formålet med støttepuljen og fellowship-programmet er ifølge Sovereign Tech Agency at understøtte det samlede digitale open source-økosystem og derigennem Tyskland og Europas digitale suverænitet, innovationskapacitet og konkurrenceevne.

Case: Slesvig-Holsten

Den tyske delstat Slesvig-Holsten har de seneste fem år arbejdet aktivt på at indføre open source-software som erstatning for proprietære løsninger fra store tech-selskaber. I 2024 installerede de LibreOffice på 30.000 PC'er, som skal fungere som ny standardapplikation i stedet for Microsoft Office.²⁸ Slesvig-Holsten har valgt en trinvis proces, så der er mulighed for at migrere processer og værktøjer til LibreOffice. Særligt skabte det udfordringer at migrere skabeloner og specialfunktioner i regneark, finde løsninger til dokumentudveksling med eksterne parter samt sikre integration med øvrige forretningsapplikationer. Derudover var der enkelte funktioner, fx OneNote, som det nye system ikke kunne levere. Delstaten har derfor anvendt ressourcer på at kode de nye programmer, så de kan tale sammen og udføre de opgaver, der skal løses. Som et næste skridt arbejder Slesvig-Holsten på at udskifte hele Windows-styresystemet med Linux. Slesvig-Holsten har implementeret en omfattende forandringsledelsesindsats for at understøtte medarbejderne i overgangen. Forandringslederne har haft særligt fokus på kommunikation, vejledning og løbende støtte i forbindelse med indførelsen af nye applikationer og arbejdsgange.

7.1.3 Schweiz

Open source er et af de tre hovedtemaer i Schweiz' digitaliseringsstrategi fra 2025, der sætter retningslinjerne for landets digitale udvikling og er bindende for den føderale administration. I strategien fastslås, at den føderale administration aktivt vil promovere brugen af open source-software for at sikre øget transparens, sikkerhed og innovation i administrationens it-systemer og ikke mindst styrke den digitale suverænitet.²⁹

I 2024 trådte den schweiziske lov "Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben" (EM BAG) i kraft.³⁰ Den schweiziske lov pålægger føderale myndigheder at gøre software, der udvikles af eller for dem, tilgængelig som open source – med undtagelse af tilfælde, hvor det ikke er muligt af hensyn til tredjepartsrettigheder, informationssikkerhed eller andre væsentlige interesser. Loven gælder udelukkende for det føderale niveau, og ikke automatisk for kantonen og kommuner, som udgør en betydelig del af den schweiziske offentlige sektor.

²⁵ [Wer wir sind: Ihr Partner für digitale Souveränität - ZenDiS | Zentrum Digitale Souveränität](#)

²⁶ [BWI und ZenDiS schließen Rahmenvertrag über souveräne Kommunikations- und Kollaborationslösungen - ZenDiS | Zentrum Digitale Souveränität](#)

²⁷ [Home | Sovereign Tech Agency](#)

²⁸ [Historien gik verden rundt, da de skrottede Microsoft: Nu fortæller tysk minister for digitalisering, hvordan open source-projektet går - Computerworld](#)

²⁹ <https://digital.swiss/userdata/uploads/strategie-dch-en.pdf>

³⁰ [New Open Source law in Switzerland | Interoperable Europe Portal](#)

Formålet med EMBAG er at fremme gennemsigtighed, sikkerhed og effektivitet i den offentlige forvaltning samt reducere afhængighed af proprietær software. Desuden giver loven mulighed for, at offentlige myndigheder kan tilbyde ydelser relateret til support, integration eller it-sikkerhed, så længe omkostninger ved ydelserne dækkes og er knyttet til varetagelse af de offentlige opgaver. Denne bestemmelse i loven bidrager til, at staten kan fremme anvendelsen af open source-software i føderale myndigheder uden at forvride markedet. Som led i implementeringen af EMBAG-loven er der etableret en koordinerende funktion under den føderale enhed for digital transformation og it-styring, som bistår myndighederne med deres anvendelse af open source-software.³¹ Her varetages flere af de opgaver, der normalt forbindes med et Open Source Program Office (OSPO), herunder fastsættelse af strategiske retningslinjer, vejledning i brug, publicering af kildekode og licenshåndtering af open source-software. Denne struktur bidrager til, at EMBAG-lovens krav om "open by default" kan realiseres på tværs af den føderale forvaltning.

7.1.4 Nederlandene

Nederlandene har gennem en årrække markeret sig som et af de lande i Europa, der ønsker at gå længst, når det gælder udbredelsen af open source-software i den offentlige sektor. Siden 2007 har indsatsen for open source været forankret med regeringens "open, unless"-princip, som fastslår, at offentlig software som skal være åben – medmindre særlige hensyn som sikkerhed eller omkostninger nødvendiggør det modsatte. Med vedtagelsen af "Open Government Act" i 2022 blev dette princip styrket yderligere, da loven fastslår, at offentligt ejet kildekode skal betragtes som generel regeringsinformation og dermed som udgangspunkt være offentligt tilgængelig ifølge national lovgivning.³²

Open source-initiativerne er især blevet drevet af det nederlandske indenrigsministerium (BZK), som i 2023 oprettede et Open Source Programme Office (OSPO) for at fremme brugen af open source på tværs af den offentlige sektor. OSPO'et understøtter implementeringen af "open, unless"-princippet gennem udvikling af en national strategi for open source, pilotprojekter for udgivelse af offentlig software samt uddannelses- og kompetenceinitiativer.³³ Derudover har OSPO'et bidraget til at mobilisere et open source-økosystem i landet gennem samarbejde med virksomheder og organisationer, som udvikler og understøtter open source-løsninger. Open source har desuden en stærk lokal forankring i Nederlandene, herunder findes der et stort engagement i den nationale kommuneforening (VNG) og et voksende netværk af offentligt ansatte, der arbejder aktivt med open source. Den høje modenhed betyder, at videndeling og erfaringsudveksling mellem offentlige enheder er i hastig udvikling og understøtter en mere effektiv og bæredygtig udbredelse af open source på alle forvaltningsniveauer i Nederlandene.

7.1.5 Frankrig

I Frankrig er offentlige myndigheder forpligtede til at fremme brugen af fri og åben software, når de udvikler, indkøber eller anvender deres informationssystemer. Dette princip er fastsat i Digital Republic Law fra 2016, som blandt andet fastslår, at software udviklet med offentlige midler i offentlige myndigheder som udgangspunkt skal udgives som open source.³⁴ Loven slår også fast, at digital suverænitet er et eksplicit mål for staten, og dermed skal offentlige myndigheder sikre, at deres informationssystemer forbliver under deres egen kontrol og understøtter bæredygtighed og teknologisk uafhængighed.

³¹ [Open Source Software \(OSS\)](#)

³² [OSS Country Intelligence Report_NL_v1.docx](#)

³³ [Open Government Action Plan 2023-2027 Open for everyone](#)

³⁴ [Main FRANCE_Report_V1_After last review.docx](#)

Som led i at fremme denne dagsorden har den franske regering etableret en statslig enhed under det interministerielle digitale direktorat, Dinum, der fungerer som et nationalt Open Source Programme Office (OSPO). OSPO'et har ansvaret for at koordinere open source-politikker, udarbejde retningslinjer og styrke videndeling om open source på tværs af den offentlige sektor. Derudover har Dinum etableret et regeringsgodkendt softwarekatalog med anbefalede open source-løsninger, som myndigheder kan bruge som alternativ til proprietær software.³⁵ Dette katalog gør det væsentligt nemmere for myndigheder at lokalisere konkrete alternativer og bidrager dermed til at omsætte principperne bag Digital Republic Law til praksis.

DINUM koordinerer derudover den franske stats sammenhængende portefølje af åbne samarbejdsværktøjer - La Suite. Formålet er at give offentligt ansatte en samlet kontorpakke baseret på open source for at styrke digital suverænitet, reducere leverandørafhængighed og lette gensidig genbrug på tværs af myndigheder. La Suite drives efter principper om, at software skal være open source, følge en fælles designlinje og køre på franske infrastrukturer. Værktøjerne udrulles gradvist til statslige ministerier og samarbejdspartnere.³⁶

Initiativet minder meget om det tyske projekt openDesk, som har samme formål: at give den offentlige sektor i Europa en mere uafhængig og bæredygtig digital arbejdsplads. Frankrig og Tyskland samarbejder om udviklingen af de to løsninger.

7.2 Tiltag fra EU og FN

EU arbejder aktivt for at fremme brugen af open source gennem en række initiativer, der skal styrke gennemsigtighed, samarbejde og digital suverænitet i medlemslandene. Et af disse tiltag er Open Source Observatory (OSOR), som fungerer som en vidensplatform, der tilbyder information og ekspertise om open source til offentlige myndigheder og andre interessenter på tværs af EU.³⁷ Derudover har EU etableret EU Open Source Solutions Catalogue, som stiller 640 open source-løsninger til rådighed for anvendelse af både myndigheder og andre aktører.

Open source-software nævnes eksplicit i centrale politiske og retlige initiativer som European Interoperability Framework (EIF), interoperabilitetsforordningen og AI-forordningen. I EIF beskrives open source-software som en nøgle til at sikre genbrug, åbenhed og sammenhæng i de digitale løsninger, som borgere og myndigheder er afhængige af. Det ses som et vigtigt redskab til at realisere visionen om en digitalt sammenhængende offentlig sektor i EU. Interoperabilitetsforordningen går skridtet videre og lægger op til, at myndigheder aktivt skal vurdere og anvende open source-løsninger, når de udvikler eller anskaffer it-systemer. Det handler ikke kun om teknisk effektivitet, men om at sikre åbenhed, langsigtet kontrol og strategisk uafhængighed i den offentlige sektor. I AI-forordningen er der også særlige krav for open source-løsninger. Forordningen stiller i en række situationer lempelige krav til udbydere af AI-løsninger, som frigives i henhold til open source-licenser, da disse AI-systemer og AI-modeller til almen brug helt eller delvist undtages fra forpligtelserne i AI-forordningen.

I EU-Kommissionens digitale strategi er der sat fokus på øget anvendelse af open source-software internt i Kommissionens egne systemer og arbejdsprocesser.³⁸ Målet er at fremme genbrug af digitale løsninger, reducere afhængigheden af proprietær software og samskabe på tværs af enheder i Kommissionen og med andre europæiske offentlige myndigheder.

³⁵ [The Interministerial Free Software Base is a set of free software recommended by the French State since 2013.](#)

³⁶ https://code.gouv.fr/fr/mission/?utm_source=chatgpt.com

³⁷ [Open Source Observatory \(OSOR\) | Interoperable Europe Portal](#)

³⁸ [European Commission Digital Strategy - European Commission](#)

Som led i EU-Kommissionens indsats for at fremme open source understøttes desuden opbygningen af European Open Source Academy (EOSA).³⁹ Det er ambitionen, at akademiet skal fungere som en europæisk platform for kapacitetsopbygning, politisk koordinering og teknologisk udvikling inden for open source-software og -hardware. Gennem netværk, uddannelsesforløb og anerkendelse af fremtrædende projekter bidrager EOSA til at styrke interoperabilitet, digital suverænitet og bæredygtige økosystemer, hvor løsninger kan vedligeholdes, videreudvikles og genbruges på tværs af medlemslandene. Derudover har EU iværksat European Digital Infrastructure Consortium (EDIC), der er en ny juridisk ramme under EU's Digital Decade Policy Programme 2030. Formålet er at gøre det muligt for medlemslande at gå sammen om at finansiere og drive store fælles digitale projekter. En af de foreslåede EDIC'er omhandler Digital Commons (DC), hvilket henviser til digitale løsninger, platforme og infrastrukturer, der udvikles i fællesskab og forvaltes som fælles goder. Det bygger på idéen om, at borgere, myndigheder, virksomheder og forskere skal kunne bruge digitale teknologier på lige vilkår, dvs. uden at være afhængige af store, private teknologivirksomheder.

Digital Commons EDIC-ansøgningen blev sendt til EU-Kommissionen i juli 2025 og forventes oprettet i efteråret 2025. Konsortiet vil i første fase koncentrere sig om udvikling af alternativer til Microsofts Officepakke, herunder openDesk i Tyskland (se afsnit om Tyskland) og La Suite i Frankrig. Senere forventes fokus at udvides til områder som cloud og kunstig intelligens. Digital Commons EDIC er etableret for at fremme udviklingen og anvendelsen af open source-software i Europa, og det er muligt for alle medlemslande at deltage i initiativet enten som observatører eller som betalende medlemmer.

Også i FN-sammenhæng arbejdes der med open source som en strategisk tilgang til digital udvikling. I 2025 har Open Source United, et praksisfællesskab etableret under FN's Digital Technology Network, udgivet en ramme for open source bestående af otte principper.⁴⁰ Med principperne lægges der vægt på, at software skal være åben som udgangspunkt, designes med henblik på genbrug og sikkerhed, og at anvendere bidrager aktivt tilbage til open source-fællesskabet. Formålet med principperne er at fremme anvendelse, udvikling og deling af open source-software globalt set og på tværs af FN-organer. I juli 2025 var 16 organisationer og virksomheder tilsluttet open source-principperne, heriblandt de ovenfor nævnte tyske ZenDis og Sovereign Tech Agency samt European Open Source Academy.

³⁹ [European Open Source Academy](#)

⁴⁰ [Sixteen Organizations Endorse the UN Open Source Principles | Office of Information and Communications Technology](#)

8. Forudsætninger

Forudsætningerne for anvendelse af open source-software varierer betydeligt afhængigt af både typen af software og formålet med anvendelsen. Fx stilles der helt andre krav til sikkerhed, hvis open source benyttes i et samfundskritisk it-system, end hvis det indgår i et mindre innovationsprojekt. Tilsvarende kan der være stor forskel på de forudsætninger, der skal være på plads, når der udvikles software til slutbrugere i desktoplaget, og de forudsætninger der skal være til stede for software i serverlaget. Derudover vil der være forskellige forudsætninger, ved at en myndighed skal dele deres open source-software (outbound), eller om den skal anvende eksisterende løsninger (inbound).

Baseret på erfaringer fra de danske myndigheder, desk research samt erfaringer fra andre lande, er der identificeret følgende væsentlige kategorier af forudsætninger for anvendelsen af open source-software i danske myndigheder.



Organisation og implementering



Support og vedligeholdelse



Sikkerhed



Licensstyring og anskaffelse



Integration til anden software



Økonomi

Forudsætningerne gennemgås nedenfor, og de forskellige nuancer inden for hver forudsætning søges udfoldet, herunder særligt skellet mellem forudsætninger forbundet med inbound og outbound open source-software.



8.1 Organisation og implementering

Der er en række krav til organisationen og dens kompetencer, når en myndighed skal anvende open source-software. Det kan være en væsentlig organisatorisk omstilling, når brugerne skal lære at anvende ny software. Tilsvarende kan det kræve, at myndigheden opbygger eller indkøber kompetencer til at opkvalificere medarbejderne, så de er i stand til at anvende softwaren. Ledelsesopbakning er en forudsætning for anvendelse af open source og i forbindelse med overgangen fra proprietær kode til open source bør det være klart for alle, hvorfor myndigheden ønsker at skifte og hvilke fordele, man forventer at få ud af det. Derudover bør der desuden være fokus på implementering og uddannelse af slutbrugere.

Myndighedernes erfaringer viser, at der er forholdsvis stor forskel på kravene til organisation og kompetencer afhængigt af, hvorvidt der implementeres open source-software på server- eller desktoplaget. For så vidt angår serverniveauet kan særligt et strategisk organisatorisk fokus bidrage til at lette

implementeringen af open source-software. I desktoplaget er softwaren i højere grad i kontakt med slutbrugeren og den enkelte sagsbehandler, hvorfor det er en forudsætning, at der sker inddragelse af slutbrugerne, at der er investeret i tilstrækkelig efteruddannelse af den enkelte medarbejder, og at myndighedens ledere er klædt på til at praktisere forandringsledelse. Erfaringerne fra Slesvig-Holsten og af gennemførte pilotforsøg i Danmark viser, at efteruddannelsesbehovet typisk ikke er omfattende, men at det omvendt heller ikke må undervurderes.⁴¹ Det gælder især ved udskiftning af software, der har stor betydning for medarbejdernes arbejdsgange, og for udvikling og implementering af software der skal anvendes af slutbrugere som borgere og virksomheder.

Myndighedernes erfaringer med at sikre de rette kompetencer til både desktop- og serverlaget viser, at myndighederne skal sikre adgang til de rette kompetencer enten internt eller via leverandører.

Hvis myndigheden går med den interne håndtering, er det en forudsætning, at den er i stand til at rekruttere og fastholde de rette kompetencer fx ved at tildele større ansvar eller sikre et fagligt miljø, der til tider kun kan opbygges i myndigheder af en vis størrelse. I nogle tilfælde kræves et højere kompetenceniveau ved brug af open source-software⁴². Det er således en forudsætning for anvendelsen af open source-software, at der investeres i en opkvalificering af medarbejdere, der skal håndtere softwaren i desktop- og serverlaget.

Ved en leverandørbåren anskaffelse er der i vid udstrækning mulighed for at kompensere for manglende it-kompetencer internt ved at outsource den samlede implementeringsopgave til den valgte leverandør. Det er dog under den forudsætning, at myndigheden har kompetencerne til at købe denne type services fra en ekstern leverandør.

8.1.1 Særligt for outbound open source

Ligesom ved inbound brug af open source-software er ledelsesopbakning en vigtig forudsætning, hvis en myndighed skal arbejde med outbound open source-software. Myndighedernes erfaringer viser, at det kræver en ekstra indsats fra myndigheden, hvis de skal deltage i udvikling og deling af open source-software. Det er blandt andet en forudsætning, at myndigheden etablerer klare processer og retningslinjer for, hvornår og hvordan kode deles, herunder licensvalg, dokumentation, test, sikkerhedstjek og kvalitetssikring.

For at opnå reel værdi og sikre langsigtet nytte, skal organisationen derudover også aktivt følge med i videreudviklingen af koden i det åbne miljø, tage relevante forbedringer og sikkerhedsrettelser til bage samt bidrage konstruktivt til fællesskabets arbejde. Det kræver organisatorisk overskud, teknisk kapacitet og en strategisk prioritering at vedligeholde og styrke relationen til open source-fællesskaber, hvis organisationen skal opnå værdi fra outbound open source. Overvågning af nye versioner, klargøring til publicering, integration af forbedringer og sikkerhedsrettelser samt løbende dialog med fællesskabet kan dog også organiseres gennem eksterne parter. Dette kan fx ske via en central OSPO-funktion, der på tværs af myndigheder håndterer denne opgave, eller gennem aftaler med en it-leverandør, som tager ansvar for at opsamle, vurdere og implementere relevante ændringer.

⁴¹ Evalueringsrapport af pilotforsøg med forskellige typer desktop-software, tilgængelig via https://web.archive.org/web/20050513224909/http://www.oio.dk/files/Desktop-evalueringsrapport_V1-2_.pdf

⁴² <https://www.kk.dk/sites/default/files/2022-10/27102022%20-%20Svar%20til%20Rasmus%20Steenberger%20vdr%20kommunens%20overvejelser%20og%20brug%20af%20open%20Source%20software.pdf>

Eksempler på tiltag, der imødekommer forudsætningen

- * Italien har opbygget en statslig OSPO, der bistår med retningslinjer, support og en platform, hvor myndigheder kan finde eksisterende open source-programmer. OSPO'en skal bidrage til at lette implementeringen og medvirke til at give det nødvendige kompetenceløft, når myndighederne skal overgå til en ny type software.
- * EU anbefaler i *Guidelines for Sustainable Open Source Communities in the Public Sector*, at myndighederne går sammen om at sikre tilstrækkelig fælles videnudveksling på tværs af myndigheder ved at oprette platforme, hvor medarbejdere med open source-kompetencer kan udveksle erfaringer⁴³.
- * Et eksempel på tiltag rettet mod implementering i desktoplaget er Slesvig-Holsten, der har gjort sig erfaringer med at mitigere udfordringer i forbindelse med overgangen til LibreOffice, hvor medarbejderne har haft meget forskellige reaktioner, men har forsøgt at afhjælpe udfordringer ved høj grad af forandringsledelse, vejledning om den nye software og gennemsigtighed om projektet.
- * Aarhus Kommune lavede tilbage i 2014 en handlingsplan, hvori de fastsatte en langsigtet målsætning for, hvordan de ville arbejde med open source-software, herunder hvordan de vil mindske brugen af løsninger, der forudsætter bestemte tredjepartsapplikationer, og sikre at nye løsninger lever op til gældende standarder⁴⁴. På den måde satte Aarhus Kommune organisatorisk retning for arbejdet med open source-software, hvilket siden er blevet underbygget af en række yderligere tiltag senest i forbindelse med budgetforliget for 2026⁴⁵.

8.2 Support og vedligeholdelse

Softwaresupport er en forudsætning for de it-løsninger, hvor der kan opstå behov for fejlfinding, træning og teknisk assistance. Det er således ikke en særskilt problematik, for hverken proprietær eller open source-software og skal være tilgængelig i varierende grad ved brugen af det meste software. Myndighedernes erfaringer er, at det er en forudsætning for anvendelsen af software, at de træffer aktiv beslutning om, hvordan supporten skal håndteres. Softwaresupporten kan håndteres af en ekstern leverandør eller internt i den pågældende myndighed. Det stiller krav til leverandøren og myndighedens modenhed, da der skal være tilstrækkelige kompetencer i organisationen.

Aktiv og løbende vedligeholdelse er en vigtig forudsætning for, at software imødekommer organisationens behov, og at fejl i softwaren minimeres. Ligesom ved softwaresupport er dette ikke en særskilt forudsætning for open source-software, da det også gælder for proprietær software. Vedligeholdelse forudsætter, at der er tilstrækkelige ressourcer tilgængelige enten i myndigheden eller ved leverandører. Hvis en myndighed vælger at lade vedligehold ske gennem et open source-fællesskab, vil det være en forudsætning, at myndigheden har kompetencerne til at vurdere og holde sig opdateret på fællesskabets vedligehold af den pågældende kode.

8.2.1 Særligt for outbound open source

Det er en forudsætning, at der er klare regler for, hvordan myndigheder kan dele software og afholde de afledte udgifter til fx support af et stykke software, hvor det ikke kun er myndighedens egne behov

⁴³ [2021 Updated Guidelines for creating sustainable OS communities_1.pdf](#)

⁴⁴ [Handlingsplan_for_OpenSource_i_Aarhus_Kommune.pdf](#)

⁴⁵ [Budget 2026](#)

til softwaren, som bliver tilgodeset. I erfaringerne fra Schweiz har de fx sikret de formelle rammer for, at myndigheder kan tilbyde ydelser relateret til support, så længe omkostninger ved ydelserne dækkes og er knyttet til varetagelse af de offentlige opgaver.

Én af de deltagende kommuner beskriver, at de som oftest ikke deler deres egenudviklede open source-software outbound, da de vurderer, at det vil komplicere videreudviklingsprocessen, hvis det bliver lagt i en OSPO. Her har kommunen en forventning til, at de vil skulle tage for stort hensyn til andre myndigheders behov i forbindelse med support, vedligehold og videreudvikling af softwaren. Domstolsstyrelsen efterspørger modsat et sted, hvor de kan dele deres udviklede software med andre myndigheder. En forudsætning for større deling af open source-software mellem myndigheder er således, at det er muligt for offentlige myndigheder at dele koden på en hensigtsmæssig måde både for dem selv og for potentielle modtagere af koden.

Yderligere er det en forudsætning, at myndigheden enten selv, gennem en leverandør eller en fælles OSPO fastlægger klart ansvar for vedligehold og support, herunder for responstider og prioriteringskriterier for ønsker til videreudvikling og vedligehold på tværs af de deltagende myndigheder. Derudover skal de sikre aktiv deltagelse i softwarens fællesskab og systematisk overvågning af fejlrettelser og sikkerhedsopdateringer.

Eksempler på tiltag, der imødekommer forudsætningen

- * I Schweiz har de opstillet faste rammer for, hvordan den enkelte myndighed kan tilbyde ydelser relateret til support på tværs af det offentlige, når de deler open source-software. Her er det udelukkende muligt at udbyde ydelser knyttet til varetagelse af offentlige opgaver.
- * OS2-samarbejdet er et eksempel på en organisation, der bistår med støtte til små myndigheder, der ikke nødvendigvis har kapaciteten til selv at håndtere fælles udvikling og efterfølgende support og vedligehold af open source-software.
- * Tyskland har etableret enheden Sovereign Tech Agency med henblik på blandt andet at understøtte decentrale open source-initiativer, som danner grundlag for yderligere anvendelse af open source-software på tværs af sektorer og stater. De har også et fellowship-program, hvor de i en tidsbegrænset periode aflønner open source-eksperter for deres arbejde med at vedligeholde open source-løsninger til gavn for alle, der anvender koden.⁴⁶

8.3 Sikkerhed

Uanset tilgangen til sikkerhed, er det et væsentligt opmærksomhedspunkt. Og brugen af open source-software kan være et skift i forhold til proprietær kode, hvor brugerne som oftest kan forvente, at de med de købte licenser også får en løsning, som er sikker, løbende holdes opdateret og fejlrettes. Derfor er det en forudsætning, at myndighederne er i stand til at vurdere open source-softwarens modenhed og sikkerhedsniveau enten ved hjælp af internt opbyggede kompetencer eller ved at indhente dem hos en tredjepart, der kan give programmet et eksternt kodereview.

For så vidt angår desktoplaget ser myndighederne primært sikkerhedsfordele ved open source-software, hvor flere øjne potentielt kan bidrage til hurtigere fejlrettelser og muligheden for at trække på et

⁴⁶ [Home | Sovereign Tech Agency](#)

bredt felt af kompetencer, hvis der er et aktivt fællesskab. Det er dog en forudsætning, at der er et aktivt fællesskab eller en kompetent organisation bag, og at myndigheden er i stand til aktivt at vurdere fællesskabet eller organisationens modenhed i forhold til at håndtere softwarens sikkerhed. Alternativt skal myndigheden hente disse kompetencer ved en tredjepart, der kan gennemføre kodereview eller har kendskab til og kan indgå i softwarens fællesskab.

8.3.1 Særligt for outbound open source

For outbound open source-software er det en forudsætning, at der ikke sker kompromittering af information, som myndigheden skal holde fortrolig. Som beskrevet i *Vejledning om offentlige myndigheders anskaffelse af open source-software*, kan dette håndteres ved, at kritisk information placeres i en separat datafil, som kaldes fra programmet og ikke stilles til rådighed sammen med koden.⁴⁷ Tilsvarende er det en forudsætning, at myndighederne indfører systematiske sikkerhedsvurderinger inden deling af kode, herunder trusselsmodellering og risikovurdering. Når koden er gjort frit tilgængelig, skal myndighederne også kunne understøtte en central sårbarhedsovervågning og håndtering af sårbarheder for open source-software-porteføljen, der er blevet gjort frit tilgængelig. Derudover skal myndigheden, ved større og forretningskritiske softwarekomponenter, koordinere respons på sikkerhedshændelser, så der reageres hurtigt og ensartet for fællesskabet. Derudover vil det være hensigtsmæssigt, hvis myndigheden ligeledes kan facilitere vidensdeling om nye trusler, sikkerhedsopdateringer og best practice. Dette kan eventuelt håndteres af en OSPO eller udliciteres til en ekstern leverandør.

Særligt for kritisk infrastruktur bør brugen af open source-software balancere åbenhedens fordele med behovet for at beskytte samfundets sikkerhed gennem fortrolig håndtering af følsomme oplysninger. Der kan således være en generel risiko ved at stille koden bag samfundskritisk software frit tilgængeligt, da det kan udstille eventuelle svagheder over for aktører med dårlige hensigter. Det vil således være en forudsætning, at myndighederne tager aktivt stilling til, hvorvidt softwaren kan deles uden, at eventuelle sårbarheder kan udnyttes.

Eksempler på tiltag, der imødekommer forudsætningen

- * De grundlæggende sikkerhedskrav, som myndigheder stiller i forbindelse med indkøb af software, er i mange tilfælde sammenlignelige, uanset om der vælges proprietær software eller open source-software. Myndigheder kan fx anvende eksisterende viden om it- og informationssikkerhed fra Staten og Kommunernes Indkøbsservice (SKI) eller anvende deres rammeaftaler.
- * I forlængelse heraf findes der en række internationalt anerkendte standarder, som myndighederne kan anvende i arbejdet med open source-software fx ISO 27001 og OpenSSF.
- * Når myndighederne skal sikre tilstrækkelige kompetencer til at håndtere sikkerheden i komponenterne, kan det ske enten ved intern kompetenceopbygning, indkøb af eksterne kompetencer ved en leverandør eller indgå i fællesskaber i stil med OS2. Det ses fx på erfaringerne fra Tyskland, hvor fælles udviklede softwareløsninger bliver stillet til rådighed på tværs af myndigheder og den enkelte myndighed derfor ikke i samme grad skal håndtere kompetenceudfordringerne.

⁴⁷ Microsoft Word - Vejledning om om offentlige myndigheders anskaffelse af open source-software [DOK501100].DOC

8.4 Licensstyring og anskaffelse

Generelt er det de samme udbudsretlige regler, der gælder for anskaffelse af open source-software som for offentlige indkøb i øvrigt. Det betyder, at hvis myndigheden ønsker at indkøbe open source-software, vil det af hensyn til gennemsigtigheden i anskaffelsen kræves, at myndigheden specificerer, hvilke open source-(mindste)krav, der stilles til softwaren. Specifikationen kan evt. ske ved at anføre, at programmet skal være licenseret via en licens, der er optaget på Open Source Initiative's liste over anerkendte open source-licenser.⁴⁸

Det er en forudsætning for myndighedernes anskaffelse af open source-software, at de har indblik i og mulighed for løbende afdække og holde sig opdateret på de relevante open source-softwareløsninger. Til forskel fra proprietær software er det i højere grad op til den enkelte myndighed at afsøge, hvilke løsninger der er tilgængelige, særligt hvis der er tale om community, intern/privat eller foundation-drevet open source-software. Derudover er det en forudsætning at myndighederne kender deres egne løsninger og behov i tilstrækkelig grad, så de er i stand til at stille de rigtige krav til leverandørerne af open source-software. En myndighed beretter, at de for nogle af deres open source-løsningers vedkommende hyrer eksterne leverandører ind til arbejdet med at kravspecifisere og følge op på om leverancerne lever op til de opstillede krav. Herved behøver myndigheden ikke i samme grad have kompetencerne til at være med helt nede i hver eneste løsning, men kan fokusere på det samlede overblik over myndighedens systemlandskab.

8.4.1 Særligt for outbound open source

Myndighedernes erfaringer viser, at der inden for licensstyring er en række særskilte forhold, som gør sig gældende, når der anvendes open source-software. Open source-licenser kan indeholde forskellige vilkår om fx, at videreudvikling ikke bare må, men også skal videregives (såkaldte copy-left vilkår), eller at programmet ikke må benyttes i kommercielle sammenhænge. Ved outbound open source-software skal ledelsen derudover være indforstået med, at softwaren deles med andre myndigheder eller stilles tilgængeligt via fx MIT-licenser. Myndighederne skal derfor være i stand til at anvende licenserne og have tilstrækkelig viden om de vilkår, der gør sig gældende, både når myndighederne køber open source-software i markedet eller vælger at egenudvikle software, som de efterfølgende vælger at gøre tilgængelig via en open source-licens. Licensstyring er en forudsætning, der kan håndteres internt i myndigheden, udliciteres til en OSPO eller ved at indkøbe eksterne kompetencer på området.

⁴⁸ [Licenses – Open Source Initiative](#)

Eksempler på tiltag, der imødekommer forudsætningen

- * Organisationer som Statens It, der leverer it-drift og services til staten, og indkøbsfællesskaber som SKI, der hjælper stat, kommuner og regioner med at udvikle indkøbsaftaler på blandt andet it, kan være en hjælp for den enkelte myndighed, da myndigheden så i mindre grad selv skal forholde sig til open source-licensstyring og -anskaffelse. Det gælder blandt andet når det kommer til open source-hyldevarer. Statens It tilbyder fx allerede i dag open source-løsninger som kontorpakken LibreOffice og videomødeløsningen JITS, som de statslige myndigheder kan tage ned fra hylden og vælge at tage i brug.
- * I regi af OS2-samarbejdet er der udarbejdet et juridisk notat om myndighedernes deltagelse i samarbejdet og anskaffelse af open source-software⁴⁹. Det gør det lettere for OS2-medlemmerne, at nødvendige juridiske afklaringer og relevant vejledning til håndtering af open source-anskaffelse og -licenser er tilgængeligt, når de skal anskaffe ny software eller dele software med andre myndigheder i samarbejdet.
- * I Frankrig, Italien, Nederlandene og Schweiz er der vedtaget lovgivning, der forpligter offentlige myndigheder til som udgangspunkt at vælge open source-software og sikre, at offentligt finansieret software gøres frit tilgængelig. Det ansporer myndighederne til at undersøge markedet for open source-løsninger, inden de igangsætter anskaffelser. Samtidig er lovgivning eller nationale open source-strategier med til at vise leverandørmarkedet, at myndighederne kommer til at efterspørge open source-løsninger, hvilket kan være med til at stimulere udbuddet.

8.5 Integration til anden software

En forudsætning for, at myndighederne kan anvende open source-software er, at det er kompatibelt med og kan integreres i myndighedens eksisterende systemlandskab. For open source-software i desktoplaget som fx en open source-kontorpakke er det således nødvendigt at undersøge, hvordan den kan indpasses i den eksisterende it-infrastruktur, om eksisterende skabeloner kan konverteres, eller der skal udvikles nye, hvordan dokumenter, formler mv. skabt i den forrige kontorpakke håndteres, hvordan krav om fx webtilgængelighed overholdes, samt hvordan dokumenter fremover udveksles med andre myndigheder og organisationer.

For open source-software i serverlaget er omfanget af integrationer og tekniske bindinger selvsagt meget afhængig af, hvilket produkt der konkret er tale om. Her vil myndigheden dog typisk skulle forholde sig til kompatibilitet og integrationer, uanset om der er tale om proprietær eller open source-software, hvorfor forskellen mellem anskaffelse af den ene eller anden type ikke er så stor.

Erfaringer fra både de danske og udenlandske myndigheder viser derfor samlet set, at det er helt centralt, at der bliver skabt et overblik over omfanget af de omkostninger og risici, der vil være forbundet med tilretning af de snitflader og integrationer, der er mellem den ønskede open source-software og omkringliggende systemer.

Integrationerne kan enten udvikles efter, at myndigheden har investeret i et stykke software, eller der kan løbende stilles krav til myndighedens leverandører om, at det udviklede software skal følge internationale standarder. Derudover kan myndighederne stille krav til, at deres it-løsninger skal kunne

⁴⁹ [Notat vedrørende OS2-fællesskabet og Open Source | OS2 – Offentligt digitaliseringsfællesskab](#)

anvendes i samspil med både proprietær og open source-software med henblik på at mindske friktionen, hvis myndigheden ønsker at skifte til en anden type software på et senere tidspunkt. Dette gør sig gældende for både proprietær og open source-software.

8.5.1 Særligt for outbound open source

Når myndigheder udvikler open source-software, vil det være en forudsætning, at softwaren følger internationale standarder og at myndigheden har kompetencerne til at holde sig opdateret og udvikle efter de fastsatte standarder.

Eksempler på tiltag, der imødekommer forudsætningen

- * Myndigheder som Aarhus Kommune og den tyske delstat Slesvig-Holsten har gjort sig værdifulde erfaringer med håndtering af integrationer i forbindelse med implementering af open source-løsninger. Erfaringsopsamling og deling af best practice herfra kan understøtte andre myndigheders implementering af de samme eller lignende open source-løsninger.
- * Erfaringer fra Aarhus Kommune viser fx, at det ved implementering af open source-kontorpakker kan være en fordel dels at foretage en teknisk bindingsanalyse af fagsystemer og dels at teste programmerne af på en mindre gruppe medarbejdere og derved undersøge, hvor der er udfordringer med at få adgang til de systemer eller løsninger, der er brug for integration til.⁵⁰
- * Større open source-satsninger på tværs af myndigheder som fx openDesk i Tyskland kan sikre fælles løsninger på de mest udbredte integrationsudfordringer for myndighederne. Tilsvarende kan open source-programkontorer på tværs af myndigheder belyse integrationsaspekter for relevant open source-software, så hver enkelt myndighed ikke skal håndtere dem alene.
- * Sundhedsdatastyrelsen har i arbejdet med Den Nationale Serviceplatform haft fokus på brugen af åbne internationale standarder, som platformen følger konsekvent. Standardiseringen sikrer bedre kommunikation mellem forskellige systemer og muliggør samtidig en effektiv integration af nye komponenter og services, både egenudviklede og open source, hvilket reducerer risikoen for tekniske udfordringer.

8.6 Økonomi

Der er ofte forskel på økonomien forbundet med proprietær og open source-software. Open source-licensen er altid gratis (når man ser bort fra det vederlag, open source-licensgiveren eller andre i rollen som leverandør måtte opkræve på tillægsydelser), mens proprietær software typisk koster penge at anskaffe. Omvendt medfølger support- og vedligeholdsydelser typisk ikke med open source-software, hvorfor myndigheden enten skal have eller opbygge kompetencerne internt, gennem et fællesskab som OS2 eller anskaffe dem hos en leverandør. Samtidig kan der ved et skifte fra proprietær software til open source-software være omkostninger til migrering, tekniske integrationer og oplæring af medarbejdere. Derfor viser myndighedernes erfaringer, at hvis myndighederne ønsker at udarbejde korrekte økonomiske sammenligninger mellem omkostningerne til proprietær og open source-software, så er det en forudsætning, at det sker på baggrund af de samlede omkostninger til softwaren over dens fulde levetid.

⁵⁰ Microsoft Word - Svar på 10 dages høringsforespørgsel fra Socialistisk Folkparti_Open Source

Eksisterende proprietære systemer, fx fra techgiganter som Microsoft, er dels præget af leverandørens mangeårige investeringer i et produkt, som kan anvendes internationalt og imødekommer brugernes behov. Samtidig har deres store udbredelse gjort, at myndigheder og andre virksomheder har investeret i sammenhæng mellem den eksisterende de facto-standard og andre systemer. Når en myndighed tager ny open source-software i brug, kan der derfor både være en forandringsomkostning i form af tekniske tilpasninger, men også i form af organisatoriske og kompetencemæssige tilpasninger, som kan føre til midlertidige produktionstab. Dertil kommer myndighedernes nuværende kontraktuelle bindinger til eksisterende software, der i mange tilfælde løber flere år ud i fremtiden. Anvendelse af ny software vil derfor skulle tænkes ind i myndighedens processer for it-anskaffelse for at undgå udgifter til parallelle licens-, support- og vedligeholdelsesfunktioner.

Case: Pilotforsøg med open source-kontorpakker i danske myndigheder fra 2004

I 2004 gennemførte Ministeriet for Videnskab, Teknologi og Udvikling i samarbejde med KL og Amtsrådsforeningen et forsøg med brug af forskellige typer desktop-software, herunder også open source-software.⁵¹ Selvom pilotforsøget fandt sted for efterhånden en del år siden, er det alligevel værdt at medtage her, da formålet specifikt var at opnå større viden om omkostninger, kvalitet samt økonomisk værdi af investeringer i hhv. proprietær og open source-desktop-software. Forsøgets resultater er derudover meget overensstemmende med erfaringer fra mere nutidige forsøg i blandt andet Slesvig-Holsten.

I forsøget sammenlignedes seks offentlige institutioners migrering til hhv. OpenOffice.org 1.1 (fem institutioner) og MS Office 2003 (én institution). Forsøget så blandt andet på regnskabstal, udvalgte arbejdsgange, brugernes tidsforbrug, brugervenlighedstests, teknisk kvalitet samt brugernes oplevelse af kvalitet. Forsøget viste blandt andet at:

- Slutbrugeruddannelse, uafhængigt af produktet, kan betale sig, idet slutbrugerressourceforbruget kan reduceres væsentligt.
- Der - specifikt for OpenOffice.org stillet over for MS Office 2003 - var en årlig licensbesparelse pr. desktop. Alle øvrige omkostningselementer, der blev målt, varierede kun marginalt.
- Udskiftning eller opgradering af kontorpakken ingen indflydelse eller effekt havde på ressourceforbruget eller produktiviteten i de analyserede arbejdsgange.

De steder hvor der er lavet pilotforsøg med open source-kontorpakker i desktoplaget, fx i Slesvig-Holsten eller det danske pilotforsøg fra 2004, har erfaringen været, at det på trods af en indledende investering i migrering, samlet set er muligt at opnå en økonomisk besparelse, da myndighederne undgår at skulle betale for licenser. Det skal dog understreges, at der er tale om pilotforsøg, der ikke nødvendigvis kan gennemføres i større skala i dansk sammenhæng med samme resultater.

Open source-software i form af kontorpakker på desktoplaget udgør dog kun en mindre del af danske myndigheders it-portefølje. Som beskrevet, udgør open source-software allerede et del- eller hovedelement i mange danske myndigheders it-systemer både i server- og desktoplaget, og her er det sjældent muligt eller relevant at tale om 1:1-udskiftninger mellem proprietære og open source-løsninger. Her er der mange andre faktorer, der spiller ind på valget af en samlet softwareløsning såsom kvalitet, sikkerhed, brugervenlighed, anskaffelsesmetode, leverandørafhængigheder, drift- og vedligehold, support og integrationer til andre systemer. Her vil det i endnu højere grad end for kontorpakkerne være nødvendigt med en grundig vurdering af de samlede omkostninger til softwaren over dens fulde levetid.

⁵¹ Evaluering af pilotforsøg med forskellige typer desktop-software, tilgængeligt via [Wayback Machine](#)

8.6.1 Særligt for outbound open source

Hvis en myndighed skal arbejde med outbound open source-software, er det en forudsætning, at den afsætter tilstrækkelig økonomi til at udvikle softwaren på en måde, så den egner sig til at blive delt. En myndighed påpegede et konkret eksempel, hvor de havde fået udviklet et stykke software, hvor leverandøren foreslog, at softwaren ville være relevant at dele. Det betød imidlertid, at der skulle investeres ekstra leverandørtimer i udviklingen for at højne kodekvaliteten med henblik på at sikre, at softwaren kunne bruges i flere forskellige sammenhænge.

Eksempler på tiltag, der imødekommer forudsætningen

- * Værktøjer som Statens business case-model kan være en hjælp i udregningen af de samlede omkostninger forbundet med et it-projekt – uanset om det drejer sig om open source- eller proprietær software.
- * I de tilfælde hvor der ikke er en relevant open source-løsning på markedet, kan det være relevant at gå sammen i et udviklingssamarbejde med andre myndigheder for at bygge den relevante løsning. Fx har OS2-samarbejdet udviklet løsningen OS2valghalla, der understøtter valgafvikling med et samlet system til at rekruttere og håndtere bemanning.
- * Både i Tyskland og Frankrig investeres der i at udvikle og implementere nationale open source-løsninger til fx kontorpakker i den offentlige administration. Herved kan nogle omkostninger forbundet med fx migration og tekniske integrationer fjernes fra den enkelte myndigheder. Andre lande som Italien har investeret i etableringen af OSPO'er, der kan skabe genbrugelige løsninger og yde rådgivning om både udvikling og indkøb af open source-software.

8.7 Opsamling

Baseret på erfaringer fra de danske myndigheder, desk research samt erfaringer fra andre lande, er der således identificeret følgende væsentlige forudsætninger for anvendelsen af open source-software i danske myndigheder.



Organisation og implementering

- Der skal være ledelsesmæssig opbakning og opbygges eller indkøbes kompetencer til at opkvalificere medarbejdere i forbindelse med transitionen til open source-software.
- Myndigheden skal være i stand til at opbygge et fagligt miljø omkring open source-softwaren.
- **Særligt for outbound:** Myndigheden skal opbygge klare retningslinjer for deling af kode, licensvalg, dokumentation, test, sikkerhedstjek og kvalitetssikring, hvis den deler softwaren.
- **Særligt for outbound:** Myndigheden skal kunne følge med i videreudviklingen af softwaren efter, at den er blevet delt.



Support og vedligeholdelse

- Det er en forudsætning for al software, at myndigheden træffer aktiv beslutning om, hvordan support og vedligeholdelse skal håndteres.
- **Særligt for outbound:** Der skal være klare regler for, hvordan myndigheder kan dele software og afledte udgifter til fx support og vedligehold, hvor det ikke kun er myndighedens egne behov, der bliver tilgodeset.



Sikkerhed

- Myndigheden skal være i stand til at vurdere softwarens modenhed og sikkerhedsniveau.
- Der skal være et aktivt fællesskab eller en kompetent organisation eller myndighed bag softwaren.
- **Særligt for outbound:** Der skal indføres systematiske sikkerhedsvurderinger inden deling af kode, og der skal kunne understøtte respons på sikkerhedshændelser ved forretningskritiske softwarekomponenter.
- **Særligt for outbound:** Myndigheden skal være i stand til at tage aktivt stilling til, hvorvidt softwaren kan deles, uden at eventuelle sårbarheder udnyttes.



Licensstyring og anskaffelse

- Det er en forudsætning, at myndighederne afdækker, hvilke relevante open source-løsninger, der er tilgængelige på markedet.
- **Særligt for outbound:** Myndighederne skal have tilstrækkelig viden om de vilkår, der gør sig gældende ved forskellige typer licenser.



Integration til anden software

- Det er en forudsætning, at softwaren er kompatibel med og kan integreres i myndighedens eksisterende systemlandskab.
- **Særligt for outbound:** Når der udvikles og deles open source-software, vil det være en forudsætning, at softwaren følger internationale standarder.



Økonomi

- Myndighederne skal være i stand til at vurdere omkostninger til softwaren over dens fulde levetid for realistisk at kunne sammenligne proprietær og open source-software.
- **Særligt for outbound:** Det er en forudsætning, at myndigheden afsætter tilstrækkelig økonomi til at udvikle softwaren, så den egner sig til at blive delt.

