
Beslutad av: Anna Eriksson, GD

Beslutsdatum: 2026-04-07

Styrdokumentägare: Avdelningschef för IT

Ärendenummer: 2026-02797

Giltig t.o.m.: 2029-03-06

Klassificerings-ID: 1.2.1 Upprätta och förändra styrdokument

Riktlinje för öppen programvara

Innehållsförteckning

Hänvisning till andra styrande dokument.....	2
Inledning	3
Syfte och målgrupp	3
Definitioner	3
Principer.....	4
Ansvar	4
Arbete med öppen programvara.....	5
Livscykelhantera öppen programvara.....	6
Anskaffa öppen programvara	6
Utveckla öppen programvara	6
Publicera öppen programvara.....	7
Hantera bidrag till öppna programvaruprojekt.....	7
Gemensamma ramar	8
Säkerhet genom hela livscykeln.....	8
Licenser och kompatibilitet	8
Dokumentation, rutiner och projekthälsa	9
Revidering av riktlinjen.....	9

Hänvisning till andra styrande dokument

- [Policy för öppen programvara](#)
- [Arbetsordning för Myndigheten för digital förvaltning](#)
- [Riktlinje för säker informationshantering](#)
- [Riktlinje för it-säkerhet](#)
- [Rutiner för hantering av allmänna handlingar](#)

Inledning

Öppen programvara är en viktig del i dagens digitala infrastruktur, omfattande system och tjänster. Genom att anskaffa, utveckla och dela öppen programvara kan Digg stärka samarbetet i offentlig sektor, öka återanvändningen av lösningar, minska leverantörsberoende och inlåsning samt skapa bättre förutsättningar för säker och transparent digital utveckling.

Diggs policy för öppen programvara anger den strategiska inriktningen för hur myndigheten ska arbeta med detta ämne. Den beskriver vilka principer och värden man eftersträvar. Den här riktlinjen förtydligar och konkretiserar policyn ytterligare. Den beskriver ramarna för hur man ska arbeta när man anskaffar, utvecklar, förvaltar och publicerar öppen programvara i den dagliga verksamheten. Den stöder efterlevnaden av interoperabilitetsregelverk¹ med de krav på öppenhet, säkerhet och återanvändbarhet som följer av det.

Syfte och målgrupp

Syftet med riktlinjen är att beskriva hur anskaffning, utveckling, bidrag och publicering av öppen programvara ska gå till, och att den ska ge stöd när beslut ska fattas i enskilda projekt och i löpande förvaltning. Samtidigt ska den bidra till att hanteringen av öppen programvara blir mer enhetlig och förutsägbar i hela myndigheten.

Som komplement till riktlinjen finns detaljerade rutiner samt stöddokument²³ - checklistor och mallar som beskriver hur olika moment ska genomföras i praktiken. Dessa innehåller exempelvis punkter för hur man väljer licenser, vilka säkerhetskriterier som ska uppfyllas, vilka dokumentationskrav och standarder som ska uppfyllas, hur man ska tänka kring olika språk och annat som behöver beaktas när man arbetar med öppna programvaruprojekt. De publiceras i samband med riktlinjerna och kommer att finnas tillgängliga även på Diggs kodsamverkansplattform.

Riktlinjen är ett internt styrdokument som omfattar samtliga medarbetare och konsulter som anskaffar eller utvecklar programvara för att utföra arbete och uppdrag på Digg. Den är uppbyggd efter två huvudflöden: att använda och anskaffa öppen programvara samt att utveckla och publicera öppen programvara. Därtill kommer gemensamma ramar; säkerhet, licenser, dokumentation, rutiner och stöddokument.

Definitioner

Öppen programvara

¹ [Interoperabilitetsförordningen \(2024/903\)](#)

² [Mallprojekt för öppen programvaruprojekt](#)

³ [Checklistor för öppen programvaruprojekt](#)

Med öppen programvara avses i dessa riktlinjer programvara som släpps under en licens som uppfyller definitionen för öppen programvara enligt Open Source Initiative (OSI).⁴ En sådan licens ger användaren rätt att använda programvaran fritt, ta del av och studera källkoden, ändra och vidareutveckla programvaran samt dela den vidare, inom den egna verksamheten och externt, oavsett syfte. I denna riktlinje används begreppet öppen programvara, i samma betydelse som öppen källkod och närliggande .

Kodsamverkansplattformar

För lagring, versionshantering och samarbete kring kod används så kallade kodsamverkansplattformar. Där utvecklas kod, ärenden hanteras och projekt kan publiceras som öppen programvara. Exempel på sådana plattformar är GitHub, GitLab, Codeberg/Forgejo. De kan antingen drivas i den egna it-miljön eller användas som molntjänster (SaaS). Se stöddokument för mer information om aktuella plattformar som används av Digg.

Principer

Följande avsnitt konkretiserar policyns principer för Diggs arbete med att anskaffa, utveckla, publicera och förvalta öppen programvara.

- Öppenhet ska vara utgångspunkten för tekniska lösningar och arbetssätt,
- Återanvändning av annan öppen programvara ska prioriteras före nyutveckling,
- Uppmuntra medarbetarna att aktivt bidra tillbaka till relevanta projekt i organisationen,
- Programvara ska hanteras med modern säkerhet under hela livscykeln.
- Vid anskaffning ska programvara som stödjer öppna format och öppna standarder föredras.
- Strategiskt arbete ska ske genom gemensamma byggstenar, agila arbetssätt och delade lösningar.

Ansvar

Arbetet med öppen programvara bygger på samma ansvarsfördelning som övrigt arbete med system och information på Digg. Avdelnings- och verksamhetsansvarig chef, det vill säga informationsägare, har ett övergripande ansvar för att policyn och denna riktlinje följs inom den egna verksamheten.

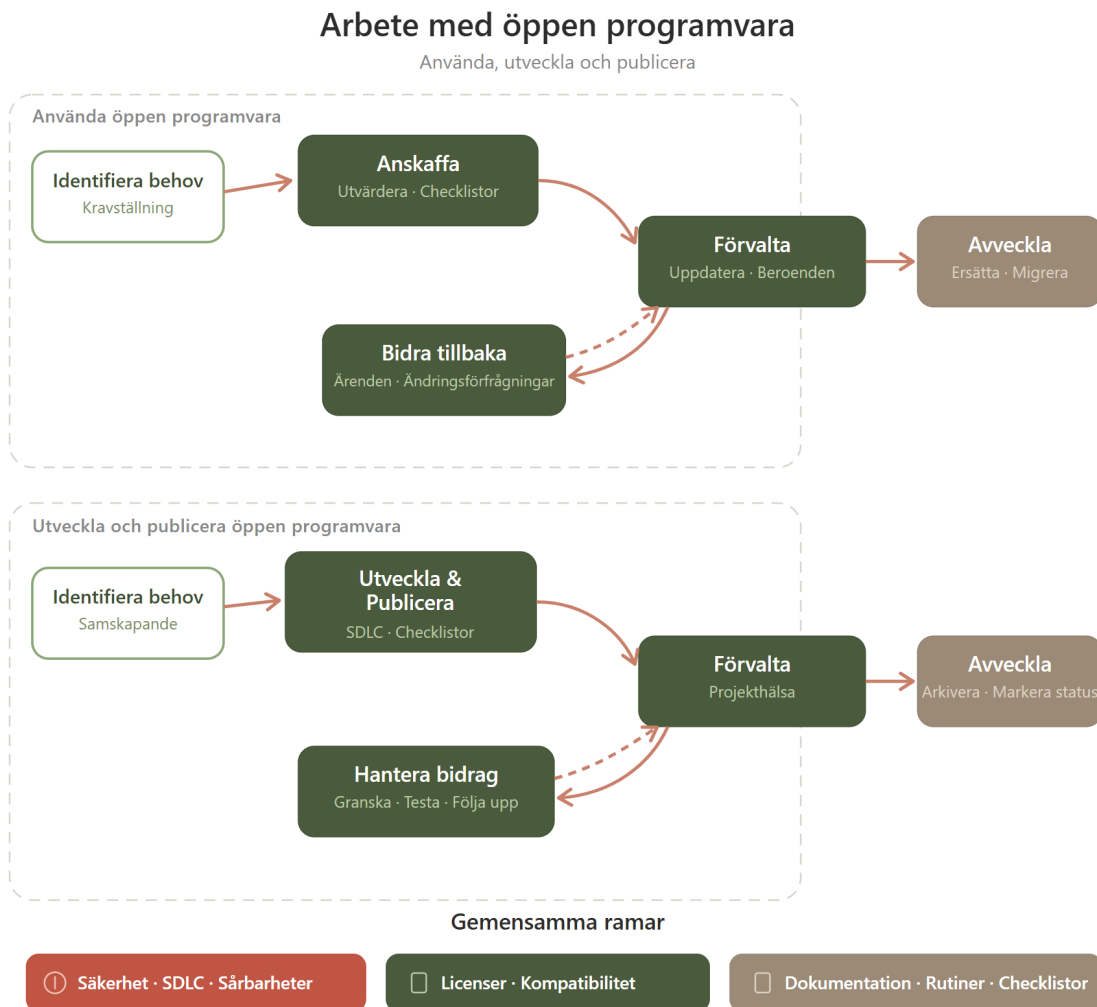
Systemägare tillika verksamhetsansvarig enhetschef ansvarar för att programvara – inklusive de delar som är öppna – hanteras i linje med riktlinjen. De ser till att det finns förvaltning, att risker följs upp och att licenser, beroenden och säkerhetsaspekter hanteras och följs upp.

⁴ [Open Source Initiative](#)

Det operativa ansvaret för ett projekt med öppen programvara ligger på ett eller flera ansvariga team. Om ett projekt berör flera informationsägare eller verksamhetsområden ska ansvarsfördelningen tydliggöras. Ansvaret innebär bland annat att man arbetar med kod, beroenden, felrapporter och förbättringsförslag, tar emot externa bidrag när det är aktuellt och håller dokumentationen uppdaterad. Utvecklare och andra tekniska roller ska följa de rutiner och mallar som finns, använda tillgängliga verktyg och uppmärksamma frågor som rör till exempel säkerhet eller licenser.

Arbete med öppen programvara

I följande avsnitt beskrivs hur Digg arbetar med öppen programvara inom centrala områden. Tillsammans ger avsnitten en samlad bild av hur Digg omsätter policyn i praktiken.



Figur 1: Översikt över två huvudflöden för arbete med öppen programvara: använda öppen programvara samt utveckla och publicera öppen programvara, med gemensamma ramar för båda flödena

Livscykelhantera öppen programvara

Öppen programvara hanteras utifrån ett livscykelperspektiv. Det innebär att man redan från behovs- och idéskedet tar ställning till hur programvaran ska användas, förvaltas och eventuellt avvecklas, samt att versionsuppdateringar sker under resans gång.

För en anskaffad it-lösning i drift ska det vara tydligt vem som ansvarar för förvaltning och uppdateringar, samt hur beroenden till andra projekt och komponenter ser ut.

När ett projekt inte längre har aktiv förvaltning ska det avslutas. För ett egenutvecklat projekt kan det till exempel innebära att projektet markeras som inaktivt/arkiverat på den kodsamverkansplattform där det ligger, att dokumentationen uppdateras och att användare informeras om statusen.

En tydlig livscykelhantering gör det enklare för Digg att använda befintliga öppna programvaruprojekt och för andra aktörer att bedöma om och hur kod från Digg kan återanvändas.

Anskaffa öppen programvara

När Digg anskaffar programvara ska öppen programvara övervägas som ett prioriterat alternativ. Det innebär att man vid kravställning och val av lösning systematiskt ska ta med aspekter som öppenhet, återanvändning, standarder och interoperabilitet.

Öppen programvara behöver i sig inte upphandlas när man anskaffar själva programvaran, däremot kan en organisation ändå genomföra en upphandling för en öppen programvara för stöd, anpassningar eller andra tjänster kopplade till den öppna programvaran, eller avropa från ett ramavtal om ett sådant finns.

Vid anskaffning av en it-lösning behöver kravställaren bedöma hur väl lösningen möter verksamhetens funktionella behov och hur den förhåller sig till informations- och it-säkerhet, befintlig it-arkitektur, öppna standarder, förvaltningsbarhet och licensvillkor. Om lösningen helt eller delvis bygger på öppen programvara ska även projektets hälsa bedömas. Det kan exempelvis ske genom att se hur aktivt projektet är, hur sårbarheter hanteras, om det finns en aktiv gemenskap eller leverantör, och hur bidrag tas om hand.

När öppen programvara inte är lämplig eller möjlig vid anskaffning ska det finnas en dokumenterad motivering.

Utveckla öppen programvara

När Digg utvecklar programvara ska det präglas av öppenhet och möjlighet för andra team, myndigheter och externa aktörer att följa arbetet och vid behov bidra till exempelvis en felrättning, eller att kunna återanvända. Källkod, dokumentation och annan nödvändig information ska successivt göras tillgänglig på vald kodsamverkansplattform.

Det innebär till exempel att felanmälningar, förbättringsförslag och andra ärenden hanteras strukturerat och synligt så länge projektet är aktivt. De som arbetar med öppen programvara behöver ha grundläggande kunskap om de etablerade arbetssätt, konventioner, metoder för säker utveckling och hanteringen av licenser som finns att förhålla sig till, och ska genom exempelvis intern utbildning eller dokumentation säkerställa att man skaffar den kompetensen.

Publicera öppen programvara

När Digg publicerar programvara som öppen programvara sker det med avsikt att den ska kunna återanvändas och skapa nytta.

Innan publicering ska ansvarigt team säkerställa att projektet går igenom ur säkerhets-, licens- och dokumentationsperspektiv. Vid behov ska relevanta funktioner inom informationssäkerhet, juridik, arkitektur och förvaltning involveras. Det ska inte finnas känslig eller skyddsvärd information i koden eller dokumentationen, licensvalet ska följa Diggs tillhörande riktlinjer, rutiner och stöddokument för licenshantering, samt vara kompatibelt med projektets beroenden. Det ska finnas en beskrivning av vad projektet är, hur det används och vilka villkor som gäller.

Det ska också framgå i projektets dokumentation eller på den valda kodsamverkansplattformen vem som ansvarar för fortsatt förvaltning och hur externa frågor och bidrag tas om hand. När ett projekt inte längre ska utvecklas aktivt är det viktigt att det framgår tydligt, till exempel genom att status markeras på kodsamverkansplattformen. På så sätt kan den som vill återanvända lösningen göra en informerad bedömning av vad det innebär att nyttja programvaran.

Detaljer om hur publicering genomförs beskrivs i stöddokumentet.

Hantera bidrag till öppna programvaruprojekt

Digg kan både bidra till befintliga öppna programvaruprojekt och ta emot bidrag till egna öppna projekt. Det minskar den interna förvaltningsbördan genom att på sikt minska behovet av egen utveckling och underhåll. Ett konkret exempel är att man istället för att underhålla ett kodbibliotek med specialanpassade programfixar, bidrar med programfixen uppströms till huvudprojektet, och därmed slipper underhålla specialanpassningen, samtidigt som programfixen kommer andra användare till gagn.

När Digg bidrar till externa projekt ska vi i första hand följa projektets etablerade arbetssätt (t.ex. ärenden (issues) och ändringsförfrågningar (merge requests/pull requests) och se till att bidraget inte innehåller känslig information som exempelvis personuppgifter eller detaljer om interna miljöer. Bidrag ska också vara förenliga med projektets licensvillkor och Diggs interna krav.

När Digg tar emot bidrag till publikt tillgängliga projekt ska det finnas tillräcklig dokumentation för att andra ska kunna bidra på ett tryggt och förutsägbart sätt (t.ex. hur man rapporterar problem och hur säkerhetsrelaterade frågor hanteras). Externa bidrag hanteras genom samma strukturerade flöden som övrig utveckling: granskning, tester och kontroll av beroenden, med omfattande

manuella och automatiserade kvalitetskontroller. Vid behov ska projektet be om kompletteringar (t.ex. tydligare beskrivning eller testfall) för att kunna göra en bra granskning. Bidrag som inte följer uppsatta rutiner, mallar, krav eller bedöms passa projektets riktning kan alltid nekas att tas in. Det finns en trend av att en del projekt får in stora och många AI-genererade bidrag, som inte alltid löser riktiga problem. Därför är det ännu viktigare än tidigare att projekt som tar emot bidrag har goda automatiska kvalitetskontroller av bidragen, och tydliga guider för att avgränsa omfattningen.

Detaljer om praktiskt genomförande för att hantera projektbidrag beskrivs i separata rutiner och stöddokument.

Gemensamma ramar

Säkerhet genom hela livscykeln

All programvaruutveckling vid Digg – oavsett om programvaran är öppen eller intern – ska följa Diggs krav på säker systemutveckling. Exempelvis innebär det att säkerhetskrav ska identifieras utifrån informationsklassning, riskanalys och tillämpliga regelverk. Arkitektur och design ska utformas med fokus på säkerhet, tydlig ansvarsfördelning och minsta möjliga attackyta. Koden ska granskas och testas, också med automatiserade tester där det är lämpligt, beroenden (bibliotek, ramverk och tredjepartskomponenter) ska bevakas och hanteras löpande utifrån sårbarheter och ändringar ska ske genom strukturerade flöden, till exempel via bidrag och kodgranskning enligt rutiner för utveckling och förvaltning. Åtkomst och ändringsbehörighet ska ges enligt principen om minsta möjliga behörighet. Data ska hanteras enligt rutiner för informationsklassning och intern eller känslig information – exempelvis personuppgifter, autentiseringsuppgifter eller detaljer om interna miljöer ska inte publiceras externt.

Rekommendationer från etablerade säkerhetsinitiativ och ramverk, såsom OpenSSF och OWASP, ska användas som stöd där det är relevant. Öppen programvara ger också, ur ett säkerhetsperspektiv, andra positiva möjligheter genom ökad insyn i vad som körs i de egna driftsmiljöerna samt insyn i hur lösningen är uppbyggd och vilka beroenden som ingår. Det underlättar granskning, riskanalys och verifiering. Tillgången till källkod möjliggör ökad rådhighet med kraften att förstärka säkerheten vid behov, till exempel genom att åtgärda sårbarheter, ändra konfigurationer eller ta bort funktioner som inte ska användas.

Mer detaljerade säkerhetsrelaterade moment beskrivs i rutiner eller checklistor.

Licenser och kompatibilitet

Licenser är en viktig del av arbetet med öppen programvara. Valet av licens för egna projekt vid publicering ska göras utifrån den inriktning som anges i policyn och projektets syfte: ibland är det viktigast att säkerställa att vidareutveckling förblir öppen, ibland att möjliggöra både öppen och sluten vidareutveckling.

När Digg bidrar till ett befintligt öppet programvaruprojekt ska Digg i normalfallet följa projektets etablerade licens, så länge den är kompatibel med myndighetens användning och krav. Allt material som publiceras av Digg som öppna projekt – både kod och dokumentation – ska ha tydlig upphovsrätts- och licensinformation så att användare enkelt kan se vad som gäller och så att licenskontroller kan automatiseras vid behov.

Licenskrav, rekommendationer och exempel beskrivs i separata rutiner och stöddokument.

Dokumentation, rutiner och projekthälsa

För att öppen programvara från Digg ska kunna användas, förstås och skapa förtroende behöver projekten vara tydligt dokumenterade och aktivt förvaltade.

Ett sådant projekt ska kunna ge betraktaren en överskådlig bild av vad lösningen gör, hur den kan användas, vilka förutsättningar som gäller för användandet och under vilka licensvillkor den tillhandahålls. Det ska också vara tydligt hur den som har frågor, vill rapportera problem eller bidra med förbättringar kan komma i kontakt med Digg eller projektet. För vissa projekt kan det dessutom vara lämpligt att beskriva hur externa bidrag hanteras, hur säkerhetsfrågor och sårbarheter ska rapporteras och vilka förhållningsregler som gäller i projektets gemenskap.

God projekthälsa handlar också om att projektet förvaltas över tid. Fel och förbättringsförslag behöver tas om hand på ett rimligt sätt, beroenden ses över och uppdateras vid behov, och dokumentation och licensinformation hålls aktuell. När ett projekt inte längre utvecklas aktivt ska det framgå tydligt så att andra aktörer kan avgöra om och hur de vill återanvända lösningen.

Som stöd för detta har Digg tagit fram mallar, exempel och checklistor för dokumentation och projekthälsa.

Revidering av riktlinjen

Denna riktlinje revideras enligt Diggs ordinarie rutiner för styrdokument.