Beleid open source software DJI

Open source software (OSS) betekent dat de broncode van bijvoorbeeld een besturingssysteem, programma of app, vrij beschikbaar is. Iedereen mag de broncode lezen, aanpassen en verspreiden. OSS speelt in het leeuwendeel van de hedendaagse technologische producten en services een onmisbare rol. Ook de Rijksoverheid stimuleert overheidsorganisaties om open source software te gebruiken, waarbij als norm geldt dat bij gelijke geschiktheid open source de voorkeur heeft.[1]

Het gebruik van OSS biedt veel voordelen maar ook aandachtspunten. Een voordeel is dat OSS vrij beschikbaar is en eenvoudig kan worden aangepast en toegepast. Aandachtspunten liggen op het vlak van de afhankelijkheid van de OSS-community als het gaat om patches, bugfixes, het onderhouden en door ontwikkelen van de software en mogelijke veiligheidsrisico's. Het is daarin niet altijd evident hoe de leveringsketen van de betreffende software georganiseerd is en welke partijen daarin een rol spelen of welke afspraken zij onderling al of niet hebben.

Dit document beschrijft het beleid van DJI ten aanzien van open source software. Voor dit document hanteren we een iteratieve aanpak waarbij het document periodiek wordt verbeterd.

Context en gehanteerde begrippen

Een korte schets van de context en de gehanteerde begrippen in het DJI beleid voor open source software:

- Open Source Software (OSS) is software waarvan de licentie aan gebruikers het recht geeft om de software – binnen bepaalde grenzen – naar eigen inzicht te gebruiken, aan te passen, te verbeteren en de broncode inclusief aanpassingen te verspreiden doordat de broncode volledig vrij beschikbaar is (bron: BZK, 2017). Aan open source software zijn geen licentiekosten verbonden (wel invoerings- en beheerskosten net als bij closed software).

- Naast de open source software zelf wordt in dit document het daarmee gebouwde resultaat, het *product*, onderscheiden.

Rationale

Van open source software is de code openbaar, wat de keuzevrijheid bevordert en "lock-in" voorkomt. Open source software maakt het eenvoudiger softwareoplossingen te hergebruiken, wat de efficiëntie verhoogt. Ook is het relatief eenvoudig en efficiënt om functionaliteit aan open source software toe te voegen, zodat deze verder kan worden gedeeld voor allerlei doeleinden, zodat iedereen ervan kan profiteren. (bron: Open source strategie EC)

[1] Recent is in de tweede kamer een motie aangenomen om 'open source, tenzij' beleid te verankeren in de Wet digitale overheid.
https://www.tweedekamer.nl/kamerstukken/moties/detail?id=2022Z10923&did=2022D22474

OSS beleid DJI

DJI volgt het Rijksbeleid waarbij overheidsorganisaties worden gestimuleerd om open source software te gebruiken. Hierbij geldt als norm dat bij gelijke geschiktheid open source de voorkeur heeft (zie ook principe AP-02 *DJI maakt zoveel mogelijk gebruik van open source oplossingen* van de applicatie visie). Bij de beoordeling van de geschiktheid wordt niet alleen de functionaliteit beoordeeld, maar worden ook niet-functionele aspecten zoals beheer, prestaties en uitvoering, beoordeeld. Een reden om de code niet openbaar te maken kan bijvoorbeeld zijn dat de broncode ongewenst inzicht geeft in de modus operandi van DJI.

Uit het SIG benchmark rapport[2] van 2022 blijkt dat acht op de tien softwareprojecten open source componenten bevatten en dat deze componenten lang niet altijd up-to-date zijn. De ervaring leert dat niet alle leveranciers daar zelf voldoende alert op zijn.

In software van leveranciers wordt in de meeste gevallen naast zelf geschreven (closed) code tevens gebruik gemaakt van open source software. Of er daadwerkelijk sprake is van het gebruik van OSS is echter niet voor alle producten en services even duidelijk zichtbaar. Daarom is, tenzij uitdrukkelijk verklaard door de leverancier dat het geleverde product of dienst geen gebruik maakt van OSS, het OSS beleid van DJI van toepassing op alle geleverde producten en diensten indien er sprake is van de levering van software[3].

Het open source software beleid van DJI stelt eisen aan het OSS-product of dienst, aan de leverancier van een OSS-product en aan DJI zelf.

Eisen aan DJI:

- DJI volgt in de basis het Rijksbeleid en maakt dus waar mogelijk gebruik van open source oplossingen. Bij de afweging wat mogelijk is worden niet alleen functionele maar ook niet-functionele aspecten zoals beheer, prestaties en uitvoering meegewogen. DJI volgt hierbij het afwegingskader dat is uitgewerkt in het rapport *Opensourcewerken* van BZK[4];
- Of er sprake is van het gebruik van OSS is niet voor alle producten en services even duidelijk zichtbaar. Daarom moet bij de selectie van producten, services en in aanbestedingen hier altijd specifiek aandacht aan worden besteed;
- DJI maakt alleen gebruik van op OSS gebaseerde producten die door een leverancier worden ondersteund;
- DJI zorgt ervoor dat de code die we gebruiken en de code die we delen, vrij is van kwetsbaarheden door voortdurende beveiligingstests uit te voeren of te laten voeren;
- DJI moet het recht hebben de code – indien nodig – openbaar te maken;
- DJI is niet alleen afnemer van OSS maar ook bereid om bij te dragen aan de community. DJI volgt hierbij het “Open tenzij” beleid vanuit het Rijk[5]. Maar dus wel op basis van een risico-, kosten- en marktafweging. Een uitwerking van hoe een bijdrage aan de community vorm krijgt, maakt deel uit van het eerste project waarvan we de code delen.

[2] https://www.softwareimprovementgroup.com/resources/2022-sig-benchmark-report/
[3] Dit geldt dus niet voor dienstverlening waarbij alleen een gebruikersrecht wordt gegeven in de vorm van een licentie.
[4] Het afwegingskader is opgenomen in hoofdstuk 3 van het rapport Opensourcewerken, BZK, 22 september 2022.
[5] Beleidsbrief vrijgeven van de broncode van overheidssoftware, Tweede kamer, 17 april 2022.

Eisen aan het OSS-product:

- de visie, architectuur en de samenhang van de onderliggende OSS componenten is beschreven;
- er is een SBOM (Software Bill Of Materials) beschikbaar waarin de toegepaste OSS componenten zijn opgenomen; bij voorkeur is de SBOM gebaseerd op standaarden zoals SPDX, CycloneDX.
- daarnaast gelden voor open source software minimaal dezelfde regels als voor het gebruik van closed source software (zie bijlage B).

Eisen aan de leverancier van het OSS-product:

- de ervaring leert dat niet alle leveranciers zelf voldoende alert zijn op het up-to-date houden van de toegepaste OSS-componenten in hun closed source software. Daarom is het (voorlopig nog) noodzakelijk is om over het actueel houden van de open source componenten specifieke afspraken te maken.
- de leverancier heeft maatregelen genomen die de kwaliteit en veiligheid van de in een product gebruikte OSS componenten garanderen gedurende de beoogde levenscyclus van het product;
- de leverancier geeft inzicht in de volledige softwareleveringsketen door afhankelijkheden tussen open source componenten in de softwareontwikkelingslevenscyclus (SDLC) te volgen met behulp van SBOM's.

Dit beleid is tevens vertaald in een aantal richtlijnen. Deze richtlijnen zijn in veel gevallen tevens van toepassing op closed source software en zelf ontwikkelde software.

Overzicht principes

Voor het gebruik van open source gelden de volgende beleidslijnen:

#	Principes
OS-01	**Voor het toepassen van open source software gelden minimaal dezelfde regels als voor het toepassen van closed source software.** Voor de kwaliteit van het applicatielandschap van DJI maakt het geen verschil of een leverancier open of closed software gebruikt.
OS-02	**DJI controleert regelmatig dat de toepassing die we gebruiken en de code die we delen, vrij is van kwetsbaarheden.** Beveiliging van een component vereist regelmatig aandacht ongeacht de fase in de levenscyclus waar deze zich in bevindt.
OS-03	**DJI is niet alleen afnemer van OSS maar draagt ook bij aan de community.** Van een overheid die gebruik maakt van open source software wordt verwacht dat ze software die zij zelf ontwikkelt of laat ontwikkelen waar mogelijk deelt met de samenleving. Dit wordt naar verwachting binnen afzienbare tijd een verplichting.

Naast de in dit document beschreven principes zijn ook enkele elders beschreven principes of richtlijnen van belang voor het open source beleid. In **bijlage A** is hiervan een opsomming gegeven.

OS-01

Nummer	OS-01
Principe	Voor het toepassen van open source software gelden minimaal dezelfde regels als voor het toepassen van closed source software.
Toelichting	Belangrijk is dat de leverancier voor open source dezelfde procedures heeft ingericht als voor zelf ontwikkelde (closed) software. De in bijlage B opgenomen eisen gelden dus zowel voor closed software en voor OSS. De leverancier moet in staat zijn een bijgewerkt product samen te stellen en hierbij (security)updates in de componenten te integreren. Bij voorkeur inclusief het automatisch genereren van een op standaarden gebaseerde SBOM (Software Bill Of Materials). Verder dient de leverancier te beschikken over een mechanisme om tijdig kwetsbaarheden in de software supply chain te signaleren en op te lossen.
Rationale	Het applicatielandschap van DJI wordt gezien als een samenwerkende keten. De kwaliteit van de keten wordt bepaald door de zwakste schakel. Daarom moeten voor open source software dezelfde eisen gelden als voor closed source software.
Implicaties	- DJI gebruikt open source software alleen wanneer een interne of externe leverancier de kwaliteit en veiligheid van de software waarborgt en bewaakt. - Leveranciers zijn in staat periodiek en op afroep automatisch gegenereerde en op standaarden gebaseerde SBOM's (Software Bill Of Materials) op te leveren. - Softwareleveranciers moeten aantoonbaar in staat zijn om systematisch gegevens over kwetsbare software componenten in de door hun geleverde producten te ontdekken, proactief te delen én deze te verhelpen. - Er moet voldaan worden aan de regels van de bijlage B Eisen aan software en software ontwikkeling. Een open source product moet aansluiten op de visie en architectuur van het DJI applicatielandschap zowel nu als in de toekomst. Inzicht in de toekomstplannen rond het open source product voorkomt onaangename verrassingen in een (te) laat stadium om adequate maatregelen te kunnen nemen.
Bron	Verwijzing naar bijlage B wordt in de toekomst vervangen door een verwijzing naar een vastgesteld document.

OS-02

Nummer	OS-02
Principe	DJI controleert regelmatig dat de toepassing die we gebruiken en de code die we delen, vrij is van kwetsbaarheden.
Toelichting	Behalve tijdens de ontwikkeling moet ook in de beheerfase periodiek worden gecontroleerd of een component nog veilig is. Deze eis is niet nieuw. Dit wordt ook elders geëist. Bijvoorbeeld in de BIO. Zo vereist BIO control 12.6.1 dat tijdig informatie over technische kwetsbaarheden wordt verkregen, dat de blootstelling van de organisatie aan dergelijke kwetsbaarheden wordt geëvalueerd en dat er passende maatregelen worden genomen om het risico dat ermee samenhangt aan te pakken. Verder vereist BIO control 18.2.3.1 dat er regelmatig controle is bij beveiligingsniveau 1 en een jaarlijkse controle bij beveiligingsniveau 2. Ook is het één van de principes van de strategie voor open source van de Europese Commissie.
Rationale	De informatiebeveiliging van een component vereist regelmatig aandacht ongeacht de fase van de levenscyclus waar deze zich in bevindt.
Implicaties	- Bij ontwikkeling en integratie van systemen wordt het principe ‘security by design’ toegepast. - Er moeten regelmatig kwetsbaarheidsanalyses of beveiligingstests worden uitgevoerd. - Naleving van beleidsregels en normen voor IB worden periodiek gecontroleerd en wanneer daarbij tekortkomingen worden geconstateerd worden die opgelost.
Bron	Open source software strategy 2020 – 2023 Think Open, European Commission, 21-10-2020.

OS-03

Nummer	OS-03
Principe	DJI is niet alleen afnemer van OSS maar draagt ook bij aan de community.
Toelichting	Indien mogelijk levert DJI ook een bijdrage aan open source software. Dit kan op twee manieren plaatsvinden: 1. het zelf open source publiceren van DJI overheidssoftware; en 2. het actief bijdragen aan open source communities en -projecten. De bij de rationale genoemde verplichting heeft betrekking op de eerste wijze. De beslissing om een component als open source beschikbaar te stellen vereist een *risicoanalyse* en een *business case*. In de *risicoanalyse* wordt bepaald of het verantwoord is de component beschikbaar te stellen. Een *business case* is noodzakelijk om een afweging te maken tussen de kosten (voor DJI) en de baten voor het Rijk en de samenleving.
Rationale	Het gebruik en het vrijgeven van open source liggen in elkaars verlengde. Van een overheid die gebruik maakt van open source software wordt verwacht dat ze software die zij zelf ontwikkelt of laat ontwikkelen waar mogelijk deelt met de samenleving. Dit wordt naar verwachting binnen afzienbare tijd een verplichting[6].

Implicaties	- DJI levert op dit moment nog nauwelijks een bijdrage. De eerste keer dat code beschikbaar wordt gesteld moet er ook op praktisch niveau wat worden uitgezocht onder meer:
	  ○ Onder wat voor licentie wordt de code beschikbaar gesteld?
	  ○ Waar en op welke wijze wordt de code beschikbaar gesteld?
	  Als de broncode eenmaal openbaar is, bepaalt de Wet hergebruik van overheidsinformatie (Who) dat overheidsorganisaties hergebruik van die code zo veel mogelijk moeten faciliteren. Dit betekent onder meer dat er een duidelijke licentie nodig is. Een voorbeeld van een dergelijke licentie is de European Union Public Licence (EUPL), een door de Europese Unie ontwikkelde licentievorm voor open source.
	- DJI moet het recht hebben om de code – indien nodig – openbaar te maken (bijvoorbeeld naar aanleiding van een Woo-verzoek);
	- Zodra het Rijksbeleid is dat er moet worden bijgedragen (vastgesteld in wetgeving) moet per component worden bepaald of deze beschikbaar kan worden gesteld.
	- Het beschikbaar stellen van open source kost ook geld.

[6] Verwacht wordt dat 'open source tenzij' wettelijk verankerd wordt in de wdo, een tweede kamer motie daartoe is al aangenomen. Verder is er nu al de beleidslijn in de 'brief Knops': "Zoals in april 2020 aan uw Kamer is gemeld, is het uitgangspunt van het kabinet dat de overheid haar broncodes vrijgeeft ('open source'), tenzij er gegronde redenen zijn om dat niet te doen". Zie ook bij *Bron*.

Bron	- Kamerbrief over vrijgeven broncode overheidssoftware, min. van BZK, 17-04-2020. - https://open.overheid.nl/repository/ronl-8746885c-59bd-4b0e-a86b-c6fa85d63c9a/1/pdf/overwegingen-bij-open-tenzij-en-aanpak-open-source.pdf - https://www.tweedekamer.nl/kamerstukken/detail?id=2022Z10923&did=2022D22474 - Rapport Opensourcewerken, BZK, 22 september 2022.

Bijlage A Overige voor open source geldende principes en richtlijnen

Naast de in dit document beschreven principes zijn ook enkele andere principes en richtlijnen van belang voor het open source beleid. In deze bijlage is een opsomming gegeven van de belangrijkste overige principes en richtlijnen die van toepassing zijn op open source:

- Non functional requirements voor open source software (document: NFRs OSS v. 0.95 – 20220609).

- AP-02 *DJI maakt zoveel mogelijk gebruik van open source oplossingen.*
  DJI volgt het Rijksbeleid dat een voorkeur aangeeft voor open source.

- AB-## *DJI maakt alleen gebruik van producten die door een leverancier worden ondersteund.*

AB-## is een algemeen business principe. Omdat de algemene business principes nog in ontwikkeling zijn is het principe voorlopig in deze bijlage opgenomen.

AB-##

Nummer	AB-##
Principe	DJI maakt alleen gebruik van producten die door een leverancier worden geleverd en ondersteund.
Toelichting	Als er een probleem is met een product, moet DJI een leverancier kunnen inschakelen om dit binnen een passend tijdsbestek op te lossen.

Bijlage B Eisen aan software en software ontwikkeling

DJI beschikt nog niet over één geïntegreerde lijst met eisen aan software en software ontwikkeling. Nu is dat nog versnipperd met eisen per onderwerp zoals BIO voor privacy en ARBIT voor de inkoopvoorwaarden.

In deze bijlage is een voorlopige opsomming opgenomen van relevante eisen aan software en software ontwikkeling.

Eisen aan software en software ontwikkeling:
- BIO
- ARBIT
- Eisen rond maatwerk:
    - 20220824 nota QAadvies DVNOplanapplicatie v096 ivm maatwerk
- CIP SSD (over normen voor secure software development).

Requirements[7]:
- Voor elk door een leverancier opgeleverd product is de visie, architectuur en de samenhang van de onderliggende OSS componenten bekend.
- De leverancier heeft maatregelen genomen die de kwaliteit en veiligheid van de in een product gebruikte OSS componenten waarborgt.
- Voor elk door een leverancier opgeleverd product is een gedetailleerd rapport (release-note) beschikbaar waarin de toegepaste OSS componenten zijn opgenomen.

Aanvullende bronnen:
- https://www.digitaleoverheid.nl/document/zobouwenwijsoftware/
- https://forumstandaardisatie.nl/publicaties/verplichte-richtlijnen-websites-en-andere-online-middelen-2019
- https://www.ncsc.nl/documenten/publicaties/2019/mei/01/beleids--en-beheersingsrichtlijnen-voor-de-ontwikkeling-van-veilige-software
- https://www.gebruikercentraal.nl/

Deze eisen gelden dus zowel voor closed als voor open software (ontwikkeling).

[7] In het beleid zijn diverse principes samengevoegd tot principe OS-01. De vervallen principes zijn hier (voorlopig) opgenomen als requirement.