Delen en hergebruik van overheidssoftware.

Juridische aspecten rondom het door de overheid ter beschikking (laten) stellen van open source software.

Opdrachtgever:
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Auteur:
Mr. Dr. M.H. Paapst

Versie	Datum		Omschrijving
0.1	24-09-2019		Eerste concept
0.2	15-11-2019		Tweede concept na bespreking opdrachtgever
1.0	03-12-2019		Definitieve versie

Inhoudsopgave

Inleiding

Steeds vaker leeft binnen de overheid de behoefte om bepaalde software aan de maatschappij of aan andere overheden beschikbaar te stellen. Denk aan projecten waar geen interne draagkracht of budget meer voor is, waarvan de leverancier end-of-life heeft aangekondigd, maar ook projecten die juist heel succesvol zijn gebleken, en waarvan het delen en vrij beschikbaar stellen enkel maar (schaal)voordelen kan opleveren voor andere overheden, voor de markt of voor de maatschappij als geheel.

Uiteraard zitten aan dergelijke beschikbaarstelling de nodige haken en ogen. Daarbij is er een verschil tussen het beschikbaar laten stellen door een ingehuurde programmeur of bedrijf, en het als overheidsorganisatie zelf beschikbaar stellen van software of broncode. Met name in dat laatste geval lijkt de Wet Markt en Overheid (hierna: Wmo) een belangrijke rol te spelen: een overheidsorgaan mag immers niet op oneerlijke wijze de concurrentie met marktpartijen aangaan. Ook zorgen over aansprakelijkheden, eigendomsrechten en compliance zijn zaken om bij stil te staan. Daarnaast is de beoogde governance van een dergelijk project van groot belang.

In deze praktische handreiking loopt u een aantal belangrijke stappen langs om met betrekking tot het zelf als open source beschikbaarstellen van software tot een weloverwogen beslissing te komen. Deze stappen zijn binnen deze handreiking opgedeeld in drie delen, namelijk:

1. Algemene keuzes;
2. Keuzes ten aanzien van het product;
3. Keuzes ten aanzien van de governance.

Onder de algemene keuzes moet worden verstaan de bestuurlijke keuzes die zijn en worden gemaakt alvorens kan worden overgegaan tot het als open source beschikbaar stellen van software. In dit hoofdstuk wordt voornamelijk ingegaan op het beleid om overheidssoftware als open source beschikbaar te stellen, op het daarbij relevante wettelijke kader, en -waar relevant- de in te roepen uitzonderingsgronden in verband met de Wmo.

Het tweede deel betreft de keuzes die moeten worden gemaakt ten aanzien van het product. Daarbij zijn verschillende onderdelen van belang. Zo moet er rekening worden gehouden met eigendomsrechten, zoals auteursrechten op software. Ook over de onderlinge aansprakelijkheidsverhouding tussen de overheid en de softwareontwikkelaar(s) dient te worden nagedacht. Daarnaast is het van belang om aandacht te besteden aan de compliance van software aan de voorwaarden voor gebruik van bestaande softwarecomponenten, geheimhouding en de AVG.

De overheid dient bij het open source beschikbaar stellen van software ook keuzes te maken ten aanzien van de governance van een dergelijk project. Dit wordt in deel drie van deze handreiking besproken. Aan de hand van deze keuzes kan vervolgens worden bepaald onder welke licentie en op welke plaats de software beschikbaar wordt gesteld.

1 Algemene keuzes

Voordat overgegaan kan worden tot het open source beschikbaar stellen van software dient rekening gehouden te worden met de relevante wettelijke kaders die in dit kader voor de overheid gelden. Daarbij is het mededingingsrecht, meer specifiek de Wmo, relevant. Door het als open source beschikbaar stellen van software mag namelijk geen oneerlijke concurrentie ontstaan met de reeds in de markt aanwezige software. Een economische activiteit is een activiteit die bestaat uit het aanbieden van goederen of diensten op een bepaalde markt. De vraag is dan of een overheidsorganisatie door het aanbieden van software en/of de broncode daarvan gezien moet worden als onderneming die een economische activiteit verricht.

1.1 Verschil tussen open source en closed source

Open Source Software (hierna: OSS) verschilt als product op belangrijke wijze van 'beperkte' software, ook wel closed source genoemd. Bij OSS draait het in de kern om de levering van broncode, met daarbij de levering van een veelomvattend ruim gebruiksrecht. Daardoor is het mogelijk om veranderingen en verbeteringen aan te brengen, en de (aangepaste of uitgebreide) software zelf verder te verspreiden. Zoals hierna nader zal worden toegelicht, creëert OSS bovendien aanvullende mogelijkheden voor hergebruik en innovatie en spaart het onnodige ontwikkelingskosten uit. Dat maakt dat de inhoud van een open source product significant verschilt van 'beperkte' software waarbij er enkel sprake is van de levering van objectcode (een uitvoerbaar bestand), onder zeer beperkende gebruiksvoorwaarden.

Naast het feit dat OSS en 'beperkte' software geen homogene producten zijn, is de doelgroep van OSS een andere. Omdat OSS vooral tot doel heeft om verbeteringen mogelijk te maken, bestaat de doelgroep niet enkel uit de medegebruikers van de software, maar vooral uit andere ontwikkelaars en marktpartijen. Voor 'beperkte' software geldt dat de eindgebruikers de voornaamste doelgroep zijn en dat het juist niet de bedoeling is dat anderen de software verspreiden, aanpassen, en daarop diensten gaan ontwikkelen.

1.2 Het algemene belang van Open Source Software

Met het aanbieden van overheidssoftware onder een open source licentie is het algemeen belang gediend. Het open source aanbieden van (mede) door, of ten behoeve van de overheid ontwikkelde software biedt namelijk een aantal belangrijke economische voordelen voor burgers, het bedrijfsleven en de maatschappij. Volgens schattingen zal voor Nederland het totale economische voordeel op 1,1 miljard euro per jaar uitkomen.[1]

Allereerst voorkomt OSS onnodige ontwikkelingskosten, zodat de algemene middelen van de overheid en de financiële middelen in het bedrijfsleven efficiënter besteed kunnen worden. Wanneer men niet twee keer het wiel hoeft uit te vinden,

[1] *Onderzoek publiceren Open Source Software. Een rapport voor: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*, Gartner 11 oktober 2017.

blijven er immers meer middelen beschikbaar voor het verbeteren van bestaande broncodes en het ontwikkelen van nieuwe software. Dit stimuleert technologische vooruitgang en biedt mogelijkheden voor het ontwikkelen van nieuwe diensten en producten naar aanleiding van nieuwe software, waardoor de economie als geheel gestimuleerd zal worden. Daarmee hangt samen dat de aanpassingsmogelijkheden bevorderend zullen zijn voor de kwaliteit van de software. Zo kunnen mogelijke problemen makkelijker worden verholpen. Bovendien zullen ontwikkelaars meer aandacht besteden aan kwaliteit, leesbaarheid en veiligheid, omdat de broncode openbaar gepubliceerd zal worden.

Ten tweede zal het als open source publiceren van broncode bijdragen aan de veiligheid van de software. Omdat andere ontwikkelaars de broncode kunnen inzien en wijzigen, kunnen eventuele veiligheidsrisico's makkelijker aan het licht komen. Weliswaar is het zo dat ook kwaadwillenden toegang kunnen krijgen tot de broncode, maar de ervaring laat zien dat publicatie van de broncode de veiligheid van de software op de langere termijn juist ten goede zal komen, bijvoorbeeld door de inzet van ethische hackers. Het verbergen van zwakke punten ("beveiliging door onbekendheid") doordat ze niet openbaar bekend worden gemaakt, is daarentegen geen geldige garantie voor de lange termijn: vroeg of laat zal iemand een achterdeurtje vinden dat mogelijk ooit zelfs opzettelijk door een ontwikkelaar is ingebouwd en verborgen.

Ten derde draagt het bij aan de verbetering van interoperabiliteit omdat overheden de software gemakkelijker op elkaar aan kunnen laten sluiten. Mede om deze reden heeft het kabinet reeds in 2007 in het Actieplan Nederland Open in Verbinding aangegeven te willen onderzoeken op welke wijze alle in eigen beheer of opdracht ontwikkelde software in beginsel onder een open source licentie is vrij te geven. Ook de Europese Commissie heeft daarom in 2017 opnieuw gepleit voor het hergebruik en het delen van open source software onder overheden.[2]

Daarnaast is het hergebruiken van broncode wenselijk in het kader van duurzaamheid. Omdat het dan niet nodig is om vergelijkbare reeds bestaande software(componenten) steeds opnieuw te ontwikkelen, bespaart OSS niet enkel financiële middelen, maar leidt het ook tot minder energieverbruik.

Tot slot zorgt het open source beschikbaar stellen van software door de overheid voor meer transparantie, doordat algoritmes en software achter overheidsbeslissingen bekend gemaakt kunnen worden. Volgens de Algemene Verordening Gegevensbescherming moet de overheid in bepaalde gevallen op verzoek ook inzicht geven in de achterliggende algoritmes bij beslissingen. Hierdoor kunnen burgers en bedrijven meer inzicht verkrijgen in de wijze waarop de overheid beslissingen neemt, wat de controleerbaarheid, en daarmee de legitimiteit, van de overheidsbeslissingen ten goede zal komen.

1.3 Is het beschikbaar stellen een economische activiteit?

In veel gevallen is het gebruik van specifieke software voor en door de overheid te beschouwen als onderdeel van de publieke taak. Denk aan het Kadaster die gratis de KLIC viewer ter beschikking stelt. De Autoriteit Consument en markt (hierna:

[2] https://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_3&format=PDF (Pagina 12)

ACM), de toezichthouder voor de Wet Markt en Overheid, heeft daarom ook aangegeven dat als het gaat om activiteiten die door bestuursorganen worden verricht, er onderscheid dient te worden gemaakt tussen de situatie waarin het bestuursorgaan handelt in de uitoefening van overheidsgezag, en de situatie waarin economische activiteiten van industriële of commerciële aard, bestaande uit het aanbieden van goederen en diensten op de markt, worden verricht. Voor zover bestuursorganen handelen in de uitoefening van overheidsgezag, verrichten zij volgens de ACM in beginsel geen economische activiteit.

Het is daarbij volgens recente jurisprudentie niet nodig dat wettelijke regels expliciet de ontwikkeling en het ter beschikking stellen van software als overheidstaak voorschrijven.[3] Ook de omstandigheid dat software met een soortgelijke functionaliteit al door een marktpartij aangeboden wordt, is in dat kader niet relevant aldus het College van Beroep voor het Bedrijfsleven, de hoogste rechter op het gebied van het economisch bestuursrecht. De door de software geboden functionaliteit dient vooral samen te hangen met, en dienstbaar te zijn aan de publieke taak. Daarbij moet gekeken worden naar het aard en het doel van de activiteiten en de regels waaraan zij zijn onderworpen. AIs van dat laatste sprake is, dan is de Wmo niet van toepassing op het beschikbaar stellen van de software, en kan vervolgens gekeken te worden op welke wijze er keuzes moeten worden gemaakt omtrent eigendomsrechten, aansprakelijkheid, bestaande componenten in de software, geheimhouding en de Algemene Verordening Gegevensbescherming (AVG). Zie hiervoor het volgende hoofdstuk.

Bij de voorgenomen keuze om software als open source beschikbaar te stellen, zou het ook kunnen voorkomen dat er sprake is van software waarvan de functionaliteit in alle redelijkheid niet samenhangt met, of dienstbaar is aan de publieke taak. Denk bijvoorbeeld aan een hele specifieke functionaliteit die enkel gebruikt kan worden binnen datacenters. Mocht dergelijke software extern worden ontwikkeld, dan kan ervoor gekozen worden om de ontwikkelende marktpartij te vragen de software als open source beschikbaar te stellen. In veel gevallen zal daar overigens ook al sprake van zijn. In de volgende hoofdstukken werken we dit verder uit.

1.4 De belangenafweging voor een Algemeen belang besluit

Pas in het geval dat bovengenoemde situaties niet van toepassing zijn, en een overheidsorganisatie zelf als onderneming een economische activiteit verricht, moet rekening worden gehouden met de Wmo, en in het bijzonder deze vier gedragsregels:

- het doorberekenen van kosten;
- het bevoordelingsverbod;
- het gegevensgebruik;
- functiescheiding.

Vooral het doorberekenen van integrale kosten stuit in juridische zin op het vereiste vanuit veel open source licenties dat de broncode bij verdere verspreiding van de

[3] ECLI:NL:CBB:2019:204

software juist kosteloos ter beschikking moet worden gesteld aan de ontvanger. Gelukkig kent de Wmo verschillende uitzonderingsgronden. Een mogelijke uitzondering is het dienen van het algemeen belang. Het beschikbaar stellen van broncode is dan een aan te wijzen activiteit die plaatsvindt in het algemeen belang als bedoeld in artikel 25h lid 5 en 6 van de Mededingingswet. Dit belang moet van geval tot geval worden bekeken en gemotiveerd, en door de overheid worden afgewogen tegen de belangen van ondernemingen. Het is daarom niet mogelijk om die afweging hier in deze handreiking alvast te maken. In algemene zin kunnen we hierover echter het volgende stellen:

Veel marktpartijen bieden open source software aan tegen vergelijkbare voorwaarden en dezelfde prijs. Deze marktpartijen verdienen hun geld door met open source producten samenhangende diensten aan te bieden. Denk aan implementatiediensten, onderhoud, doorontwikkeling en trainingen. Het door of namens de Nederlandse overheid vrij beschikbaar stellen van broncode heeft geen nadelige effecten voor deze marktpartijen, omdat zij op zichzelf niet verdienen aan het open source aanbieden van software. Daarnaast kan het gratis beschikbaar stellen van broncode juist de activiteiten van marktpartijen stimuleren. Dit omdat de marktpartijen toegang hebben de broncode en deze kunnen verbeteren, de veiligheid daarvan vergroten en eventuele problemen kunnen oplossen. Zo dragen alle marktpartijen bij aan de kwaliteit en innovatie van open source producten en kunnen ze hun eigen dienstverlening verbeteren. Dit is uiteraard gunstig voor alle partijen die op deze markt actief zijn. Ook toetreders zullen, door vrij gebruik te kunnen maken van de beschikbare broncodes, sneller nieuwe diensten kunnen ontwikkelen.

Verder is het van belang om in de afweging mee te nemen dat het beneden de kostprijs aanbieden van de broncode noodzakelijk is om de algemene belangen te dienen. Als de overheid broncodes zou moeten aanbieden tegen de integrale kostprijs, zal het opwerpen van die drempel geen extra positieve effecten hebben op de economie. Doordat er dan minder afnemers zullen zijn, zal het economische potentieel van hergebruik en innovatie niet of niet volledig worden benut. Ook de andere doelstellingen, zoals het uitsparen van ontwikkelingskosten, zullen in mindere mate of zelfs helemaal niet worden bereikt.

Naast deze noodzakelijkheidstoets is vereist te onderzoeken of de marktpartijen zelf niet in staat zijn om met hun aanbod en voorwaarden het algemene belang te dienen. Voor het bereiken van de eerdergenoemde doelen is het gunstiger dat er zoveel mogelijk aanbieders op de markt actief zijn. De doelstellingen zullen enkel kunnen worden bereikt, indien het aanbod en de variëteit zo groot mogelijk is: hoe meer bedrijven en organisaties OSS aanbieden, hoe meer kansen dat biedt voor anderen om elkaars software te verbeteren en daarop (commerciële) diensten te ontwikkelen. Vandaar ook dat vanuit heel Europa overheidsorganisaties hun broncodes vrij beschikbaar stellen. Het toetreden van de Nederlandse overheid tot de markt voor OSS draagt zodoende bij aan het bereiken van de doelstellingen.

2 Keuzes ten aanzien van product

De tweede stap in deze handreiking is het maken van keuzes omtrent eigendomsrechten, aansprakelijkheid, bestaande componenten in de software, geheimhouding en de AVG. In dit hoofdstuk worden deze keuzes uiteengezet, aangevuld met praktische voorbeelden.

2.1 Eigendomsrechten

Bij de keuzes ten aanzien van een specifiek product is het allereerst van belang om te inventariseren waar de eigendomsrechten op de software liggen. De belangrijkste vraag bij deze inventarisatie is: 'Wie bezit de auteursrechten?'. Op software rust namelijk auteursrecht (copyright). Dit houdt in dat de maker, of zijn rechtverkrijgende, het exclusieve recht heeft om de software openbaar te maken en te verveelvoudigen. De vraag wie auteursrechthebbende is van de software is bij het als open source beschikbaar stellen van deze software dan ook van groot belang. Dit heeft als reden dat de software ter beschikking wordt gesteld aan publiek, en daarmee dus in auteursrechtelijke zin openbaar wordt gemaakt. Daarnaast wordt de software gebruikt en aangepast, wat een auteursrechtelijk relevante verveelvoudiging oplevert.

In §2.1 worden handvaten gegeven hoe geïnventariseerd kan worden waar de auteursrechten op software liggen. Ook biedt deze paragraaf handvaten voor de keuzes die kunnen worden gemaakt ten aanzien van deze eigendomsrechten.

2.1.1 Auteursrecht op software

Het auteursrecht geeft bescherming aan de maker van een "werk", indien het werk:

- een eigen oorspronkelijk karakter heeft;
- het persoonlijke stempel van de maker draagt;
- voor zintuigelijke waarneming vatbaar is.

De maker is degene wiens creativiteit is terug te vinden in het werk.

Uit artikel 10 lid 1 sub 12 van de Auteurswet blijkt dat computerprogramma's en het voorbereidende materiaal ook als werk in de zin van de Auteurswet gezien kunnen worden. Daarom geldt ook voor software dat aan de hierboven genoemde voorwaarden voor auteursrechtelijke bescherming moet worden voldaan. Het is algemeen aanvaard dat het auteursrecht op software zich zowel uitstrekt over de broncode van de software, als over de 'vertaalde' vormen van de software, zoals de objectcode. De ideeën en beginselen die aan de software ten grondslag liggen worden echter niet auteursrechtelijk beschermd, nu deze niet zintuigelijk waarneembaar zijn. Een dergelijke bescherming is alleen mogelijk door middel van een octrooi.

Het auteursrecht op een werk ontstaat van rechtswege. Dit betekent dat het auteursrecht automatisch ontstaat wanneer aan de voorwaarden voor bescherming is voldaan. Er gelden geen formele vereisten, zoals registratie.

De bescherming onder het auteursrecht krijgt zijn uitwerking in het verlenen van zogenaamde exploitatierechten aan de maker of dienst rechtverkrijgende. Deze

exploitatierechten het uitsluitende recht om een werk openbaar te maken en/of te verveelvoudigen.

Verveelvoudigen is het kopiëren van een werk. Hieronder valt ook het bewerken of nabootsen in gewijzigde vorm van een werk, wanneer de creatieve keuzes van de maker zijn overgenomen. Het speciale softwareregime in de Auteurswet geeft een vergaande auteursrechtelijke bescherming aan software.

2.1.2 Borgen van rechten

Wanneer software is geselecteerd voor vrijgave, moet worden geïnventariseerd wie de auteursrechthebbende is van deze software. Uitgangspunt in het auteursrecht is namelijk dat de maker van een werk de auteursrechthebbende is. Wanneer de software meerdere makers heeft, zijn deze makers mede-auteursrechthebbende.

Om als overheid over te kunnen gaan op het open source publiceren van software, is het van belang dat de overheid auteursrechthebbende is of daarvoor toestemming heeft van de auteursrechthebbende(n), bijvoorbeeld door middel van (open source) licentie. Alleen dan is de overheid zelf gerechtigd tot het openbaar maken en verveelvoudigen van de software.

Werkgeversauteursrecht

Software kan intern door een werknemer van de overheid zijn gemaakt. Wanneer deze werknemer de software in dienstverband onder werktijd heeft gemaakt en dit behoort tot zijn taakomschrijving, dan liggen de auteursrechten van rechtswege bij de overheid op grond van het werkgeversauteursrecht (artikel 7 Auteurswet). Dit werkgeversauteursrecht is ook van toepassing op ambtenaren. Wanneer de overheid op grond van het werkgeversauteursrecht auteursrechthebbende is van de software, dan is vrijgave van de software auteursrechtelijk gezien geen probleem.

Contractuele verhoudingen

In veel gevallen zullen er echter externe partijen betrokken zijn bij het maken van software. Het zal dan afhangen van de toepassing van inkoopvoorwaarden en andere gemaakte contractuele afspraken. Deze bepalen of de auteursrechten bij de overheid liggen of dat de overheid toestemming heeft van de auteursrechthebbende(n) tot (her)gebruik van de software.

Voor een groot deel van de overheid zijn een van de volgende drie sets inkoopvoorwaarden van belang: Arbit, Arvodi en Gibit. Wanneer de overheid een overeenkomst is aangegaan met een derde waarin zij de opdracht heeft gegeven tot het ontwikkelen van software, kunnen deze inkoopvoorwaarden van toepassing zijn verklaard. In deze voorwaarden zijn onder andere bepalingen opgenomen ten aanzien van aan wie het auteursrecht toekomt op de ontwikkelde software. Het is dus van belang om na te gaan of een set van deze inkoopvoorwaarden van toepassing is verklaard op de overeenkomst met een derde tot het ontwikkelen van software.

De Algemene Rijksvoorwaarden voor het verstrekken van opdrachten tot het verrichten van diensten (ARVODI-2018) zijn algemene voorwaarden voor dienstverleningsovereenkomsten tussen de Staat der Nederlanden en derden. De Algemene Rijksvoorwaarden bij IT-overeenkomsten (ARBIT-2018) zijn algemene voorwaarden bij IT-overeenkomsten. De ARVODI-2018 en de ARBIT-2018 zijn

algemene inkoopvoorwaarden die rijksbreed zijn vastgesteld. Voor gemeenten zijn de Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT) vastgesteld.

De bepalingen uit de ARBIT-2018 (artikel 8), ARVODI-2018 (artikel 24) en de GIBIT (artikel 17) bepalen dat de auteursrechten bij de overheid (opdrachtgever) komen te liggen. Dit ligt echter anders wanneer in de software reeds bestaande componenten zijn gebruikt. In die gevallen dient de ontwikkelaar van de software (derde) een eeuwigdurend en onherroepelijk gebruiksrecht te verlenen aan de overheid. Daarbij is het van belang om na te gaan wat onder het gebruiksrecht van de software valt. Hier wordt in §2.1.3 dieper op ingegaan.

Of een van deze sets inkoopvoorwaarden van toepassing is op de overeenkomst van de overheid met een derde tot het ontwikkelen van software, moet worden uitgezocht en gedocumenteerd. Aan de hand daarvan kan worden bepaald of de overheid auteursrechthebbende is of dat zij een gebruiksrecht heeft verkregen op de software. Wanneer de overheid een gebruiksrecht heeft verkregen is het van belang na te gaan of het open source beschikbaar stellen van de software ook onder rechtmatig gebruik van de software valt. Ook zijn maatwerkafspraken mogelijk. Deze worden contractueel bedongen in de overeenkomst. (Eventuele) afwijkingen dienen dan ook goed in kaart te worden gebracht.

<u>Geen afspraken?</u>
Wanneer de auteursrechten op (een deel van) software (nog) niet bij de overheid zelf liggen, zijn er drie opties.

1. *Auteursrechtoverdracht*: De auteursrechten worden alsnog overgenomen door de overheid.

Het auteursrecht kan worden overgedragen. Deze overdracht van auteursrecht moet in een schriftelijk stuk (akte) worden vastgelegd. Aan de overdracht kunnen (financiële) voorwaarden worden gesteld, die duidelijk in de akte aangegeven moeten worden.

De overdracht van het auteursrecht gebeurt door middel van een schriftelijke akte. Deze akte moet worden ondertekend. In deze akte moet worden vastgelegd wat er precies wordt overgedragen. Het moet dus duidelijk zijn om welk werk het gaat, welke rechten worden overgedragen en onder welke voorwaarden het werk wordt overgedragen. Wat betreft overdracht is het ook van belang om afspraken te maken met betrekking tot de persoonlijkheidsrechten van de maker (zie §2.1.3).

> *Voorbeeldbepaling: [maker van het werk] draagt hierbij zijn auteursrechten in hun meest volledige omvang ten aanzien van het werk over aan de [overheid], welke overdracht [overheid] aanvaardt. Deze overdracht omvat alle tot het auteursrecht behorende bevoegdheden voor alle landen ter wereld, voor alle exploitatievormen en voor alle distributiemedia. Deze bevoegdheden betreffen, voor zover mogelijk, tevens die exploitatievormen en media die in de toekomst mogelijk zijn of worden.*

Dit alles vereist maatwerkonderhandelingen, waarbij de leverancier van de software vrij is dit te weigeren. De prijs kan hierdoor hoog uitpakken.

Een alternatief is de licentieverlening:

2. *Licentieverlening*: Aan de overheid wordt een licentie verleend die de herverspreiding en verdere bewerking toestaat.

Ook kan/kunnen auteursrechthebbende(n) een licentie verlenen aan de overheid. Dit betekent dat de auteursrechthebbende(n), onder voorwaarden, toestemming verlenen aan de overheid tot het exploiteren van de software.

Licentieverlening kan goedkoper uitvallen dan auteursrechtoverdracht, maar laat het eigendom van de auteursrechten bij de derde. Dit vormt een zeker risico wanneer dit eigendom ooit overgaat op een ander, zoals bij faillissement. Deze situatie is dan ook niet wenselijk.

Daarnaast is het bij licentieverlening van belang dat de licentie eeuwigdurend en onherroepelijk is. Wanneer dit niet het geval is bestaat het risico dat licenties kunnen aflopen of kunnen worden ingetrokken. Dit brengt onzekerheid met zich mee voor de overheid. Dit in tegenstelling tot auteursrechtoverdracht, waar de exploitatierechten niet kunnen aflopen of worden ingetrokken. Auteursrechtoverdracht is dan ook wenselijker dan licentieverlening.

Wanneer toch wordt gekozen voor licentieverlening kan gebruik worden gemaakt van de volgende voorbeeldbepaling om ervoor te zorgen dat de toestemming eeuwigdurend en onherroepelijk is:

> *Voorbeeldbepaling: [maker van het werk] verleent een eeuwigdurende, niet-opzegbare, onbeperkte en niet-exclusieve licentie tot exploitatie van het werk aan [overheid].*

Vervolgens is het onder de voorwaarden van de licentieverlening van belang dat herverspreiding door de overheid is toegestaan.

> *Voorbeeldbepaling: onder het gebruiksrecht valt in ieder geval het recht om het auteursrechtelijk beschermde werk zonder enige beperking of begrenzing met betrekking tot plek, apparatuur, tijdsduur of anderszins te gebruiken waaronder begrepen het gebruik daarvan door derden ten behoeve van [overheid].*

Zie §2.1.3 wanneer de software als open source is ontwikkeld.

3. *Opnieuw ontwikkelen*: De relevante onderdelen van de software opnieuw ontwikkelen.

Wanneer relevante onderdelen in software zitten waar de overheid geen auteursrechthebbende van is, kan een optie zijn om deze relevante onderdelen opnieuw te ontwikkelen. Deze optie kan goedkoper zijn dan auteursrechtoverdracht, maar kost tijd en kostbare capaciteit van ontwikkelaars.

2.1.3 De open source auteursrecht-licentie

Ook is het mogelijk dat de software door een leverancier als open source is ontwikkeld en/of wordt aangeboden aan de overheid. Daarbij kan van de leverancier ook gevraagd worden of hij zelf wil zorgdragen voor de governance en het beschikbaar stellen in een openbare repository. Dit maakt ook het door de overheid opnieuw beschikbaar stellen van het resultaat vaak minder complex; OSS-licenties staan immers toe dat gebruikers de software zelf ook weer aan derden beschikbaar mogen stellen.

Het centrale idee van OSS is gebaseerd op licentievoorwaarden, die erg veel toestaan aan een licentienemer. Zo mag er in de meeste gevallen geen licentievergoeding worden gevraagd, moet de broncode vrij beschikbaar zijn en moet het zijn toegestaan deze broncode vrij aan te passen en verder te verspreiden.

In veel open source-licenties (hierna: OSS-licenties) zijn bepalingen opgenomen die de verveelvoudiging en bewerking van het werk door de licentienemer toestaan, mits deze verveelvoudiging of bewerking onder dezelfde licentie blijft vallen. Dit noemt men ook wel copyleft. Ook worden in de licentie vaak vrijwaringen en bepalingen met beperkingen voor verder commercieel gebruik opgenomen.

Desondanks is ook hier elk gebruik dat buiten de in de OSS-licentie aangegeven grenzen valt, en daarmee niet voldoet aan de door de auteursrechthebbende gestelde voorwaarden, een inbreuk op het auteursrecht. Ook in dit geval moet dus goed nagegaan worden welke partijen licentiegever zijn, of de gegeven OSS-licentie adequaat is en welke consequenties deze licentie met zich meebrengt.

Ook kunnen bestaande componenten in software zijn gebruikt die onder een (OSS-) licentie vallen. Lees hierover meer in *§*2.3.1.

2.1.4 Persoonlijkheidsrechten

Naast dat de auteursrechthebbende het exclusieve recht heeft om het werk openbaar te maken en te verveelvoudigen, heeft de maker van het werk zogenoemde persoonlijkheidsrechten. Deze rechten geven de maker van het werk het recht om bezwaar te maken tegen bepaalde openbaarmakingen van zijn werk.

> *Zo kan de maker van software op grond van zijn persoonlijkheidsrechten onder andere optreden tegen openbaarmaking van zijn werk zonder naamsvermelding.*

Persoonlijkheidsrechten zijn niet overdraagbaar. Wel kan de maker voor een deel afstand doen van zijn rechten.

> *Waar bijvoorbeeld geen afstand van kan worden gedaan is het recht op bezwaar tegen misvorming, verminking of aantasting van het werk wat nadeel toebrengt aan de eer of de naam van de maker.*

Het is van belang om bij het open source beschikbaar stellen van software rekening te houden met deze persoonlijkheidsrechten. Anders bestaat het risico dat de maker van de software zich kan verzetten tegen het open source publiceren van die software. Dit geldt zelfs in het geval dat de auteursrechten zijn overgedragen aan de overheid. Het contractueel vastleggen dat de maker onherroepelijk afstand doet van

zijn persoonlijkheidsrechten, voor zover dit is toegestaan, kan voorkomen dat de maker zich hierop beroept. De overheid dient dit dan ook goed te regelen met de makers van software.

> *Voorbeeldbepaling: [naam maker van het werk] doet – voor zover rechtens toegestaan – afstand van zijn persoonlijkheidsrechten ten aanzien van het werk.*

Indien de ARBIT-2018, ARVODI-2018 of GIBIT van toepassing zijn verklaard op de overeenkomst met de maker van de software, dan is de afstand van de persoonlijkheidsrechten (voor zover rechtens toegestaan) reeds overeengekomen.

Indien ervoor is gekozen om de ontwikkelaar de software zelf te laten publiceren als OSS, bijvoorbeeld onder de EUPL-licentie, dan is deze problematiek ook ondervangen. Deze licentievorm zal verderop nog worden besproken.

2.2 Aansprakelijkheid

Alvorens we toekomen aan een bespreking van de mogelijke aansprakelijkheid die zich kan voordoen bij het (laten) beschikbaar stellen van de broncode, is het zaak om een stap terug te nemen en in te gaan op de aansprakelijkheidsregels tussen de overheid en de ontwikkelaar van software.

2.2.1 ARBIT-2018, ARVODI-2018 & GIBIT

De rechtsverhouding tussen de overheid als opdrachtgever en de ontwikkelaar van software is geregeld in de GIBIT, ARBIT-2018 en/of de ARVODI-2018, mits deze van toepassing zijn verklaard op de overeenkomst tussen deze partijen. Daarbovenop komen nog de afzonderlijke afspraken uit de overeenkomst. Deze drie sets voorwaarden bepalen als hoofdregel dat de partij die toerekenbaar tekortkomt in de nakoming van de overeenkomst, tegenover de ander aansprakelijk is voor schade. Hoewel deze hoofdregel niet afwijkt van de wettelijke regeling van 6:74 BW, kennen alle drie de regelingen een beperkingensysteem en zijn er specifieke bepalingen over de aansprakelijkheidsverdeling tussen beide contractspartijen.

De Nederland ICT-voorwaarden vallen buiten het bereik van deze handreiking. Mochten deze voorwaarden van toepassing zijn op de overeenkomst, dan is het raadzaam om aanvullend juridisch advies in te winnen.

GIBIT: de aansprakelijkheidsverdeling

Bij het bepalen of er sprake is van toerekenbaar tekortkomen in de nakoming van verplichtingen uit de overeenkomst, is het relevant welke garanties de opdrachtnemer geeft ten aanzien van de software. Deze garanties staan genoemd in artikel 10 GIBIT. De ontwikkelaar garandeert dat het product de overeengekomen eigenschappen zal bevatten en voldoet aan het overeengekomen gebruik, dat er voldoende gekwalificeerd personeel zal worden ingezet en dat hij ten minste twee jaar na datum van de acceptatie onderhoud zal plegen. Zo zal de opdrachtnemer ervoor zorgen dat het product blijft voldoen aan de regelgeving, dat het geschikt blijft voor gegevensuitwisseling met de rest van het systeem, dat het blijft voldoen aan de gemeentelijke ICT-kwaliteitsnormen en dat de performance gelijk blijft na updates. Ook garandeert de opdrachtnemer dat het product geen inbreuk maakt op intellectuele eigendomsrechten of andere rechten van derden, zoals later aan de orde zal komen in §2.2.4. Mochten deze garanties niet worden waargemaakt, dan komt de opdrachtnemer tekort in het nakomen van de overeenkomst.

Naast deze garanties kent de GIBIT een aantal bedingen waarin de aansprakelijkheid bij de ontwikkelaar wordt neergelegd. Zo vrijwaart hij de opdrachtgever van boetes van toezichthouders, voor zover die rechtstreeks verband houden met de tekortkoming van de opdrachtnemer. Hierop zijn de hierna te noemen beperkingen van de aansprakelijkheid niet van toepassing. Ook voor verplichtingen ten aanzien van het personeel van de opdrachtnemer geldt dat hij hier zelf voor verantwoordelijk is. Tot slot is de opdrachtnemer aansprakelijk voor de door de opdrachtgever te lijden en geleden schade, indien het product voor de tweede keer tijdens de acceptatieperiode is afgekeurd vanwege gebreken.

Ter beperking van de aansprakelijkheid van de opdrachtnemer, bepaalt artikel 19 lid 5 GIBIT dat gebreken die zijn veroorzaakt door fouten in derdenprogrammatuur niet als gebrek worden beschouwd in het kader van de overeenkomst tussen de

ontwikkelaar en de overheid. De ontwikkelaar is daarvoor niet verantwoordelijk, tenzij hij die fout had behoren te kennen en het effect van de fout redelijkerwijs had kunnen vermijden. Wanneer derdenprogrammatuur in de software aanwezig is, is het ook belangrijk aansprakelijkheid voor inbreuken op intellectuele eigendomsrechten van derden uit te sluiten. Zoals we in §2.2.4 zullen zien, komt het voor rekening van de opdrachtnemer wanneer het op dat punt misgaat.

GIBIT: de schadevergoedingsverplichting

In het kader van aansprakelijkheid is artikel 13 GIBIT het belangrijkste artikel. Dit artikel kent twee begrenzingen van de aansprakelijkheid. Ten eerste somt het tweede lid limitatief de schadeposten op die voor vergoeding in aanmerking komen:

- Schade aan de geleverde software of gegevensbestanden;
- Schade aan andere eigendommen van de contractspartijen of derden;
- De kosten van noodzakelijke wijzigingen in de software die zijn aangebracht ter beperking of herstel van schade;
- De kosten van noodvoorzieningen en kosten van het noodgedwongen operationeel houden van oude systemen;
- Kosten van het niet kunnen inzetten van medewerkers, goederen en faciliteiten;
- Kosten voor het herstel van gebreken van de opdrachtgever of door hem ingeschakelde derden;
- Aan derden verschuldigde vergoedingen en boetes;
- Redelijke kosten ter beperking of voorkoming van schade;
- Redelijke kosten ter vaststelling van de schadeoorzaak, aansprakelijkheid en de hoogte van de schade.

Uit deze opsomming kunnen we afleiden dat ook schade die door derden wordt geleden en op een van de partijen wordt verhaald, binnen het bereik van de rechtsverhouding tussen de contractspartijen valt. Zij kunnen elkaar aansprakelijk stellen voor deze schade.

De in lid 2 genoemde beperkingen gelden niet in alle gevallen. Wanneer derden aanspraak hebben op schadevergoeding uit letsel of overlijden, in geval van opzet of grove schuld aan de zijde van de andere partij of diens personeel en in geval van schending van intellectuele eigendomsrechten zijn deze beperkingen niet van toepassing.

Ten tweede kent artikel 13 een beperking van het schadebedrag. De aansprakelijkheid is per gebeurtenis beperkt tot vier keer de hoogte van de vergoeding die betaald is. Daarbij zal de aansprakelijkheid zich uitstrekken tot maximaal vijf miljoen euro.

ARBIT-2018: De aansprakelijkheidsverdeling

Net als de GIBIT bepaalt de ARBIT-2018 dat de opdrachtnemer een aantal verantwoordelijkheden heeft en een aantal garanties biedt. Zo garandeert hij dat hij voldoende gekwalificeerd personeel inzet dat niet werkzaam is voor een ander waardoor een belangenconflict zal ontstaan, dat hij gedurende 12 maanden na acceptatie gebreken zal herstellen en dat hij het product tot 5 jaar na acceptatie zal kunnen onderhouden (artikel 12 ARBIT-2018). In tegenstelling tot de GIBIT, bepaalt de ARBIT-2018 niet uitdrukkelijk dat de opdrachtnemer verantwoordelijk is voor

door toezichthouders opgelegde boetes, wanneer deze boetes verband houden met een tekortkoming van de opdrachtnemer.

Een aantal van de verplichtingen die uit de ARBIT-2018 voortvloeien, blijven na het einde van de overeenkomst bestaan. Dit zijn onder andere de bepalingen over vrijwaring voor schending van intellectuele eigendomsrechten, garanties, aansprakelijkheid, geheimhouding, geschillen en toepasselijk recht (artikel 34 ARBIT-2018).

ARBIT-2018: de schadevergoedingsverplichting

De verplichting tot het betalen van schadevergoeding is uitgewerkt in artikel 26 ARBIT-2018. In tegenstelling tot artikel 13 GIBIT heeft dit artikel geen limitatieve opsomming van schadeposten die voor vergoeding in aanmerking kunnen komen. Wel kent artikel 26 ARBIT-2018 een beperking van het bedrag van de schadevergoeding. Voor personen- en zaakschade wordt maximaal €1.250.000,- vergoed per schadeveroorzakende gebeurtenis. Voor andere schade geldt dat de aansprakelijke partij maximaal vier keer de hoogte van de voor de software betaalde vergoeding moet betalen.

Net als de GIBIT, geeft de ARBIT-2018 een aantal uitzonderingen op deze beperkingen. Aanspraken van derden op schadevergoeding vanwege letsel of overlijden, opzet of grove schuld aan de zijde van de wederpartij of diens personeel, schending van intellectuele eigendomsrechten en aanspraken op schadevergoeding en door toezichthouders opgelegde boetes in het kader van een tussen partijen afgesloten overeenkomst betreffende het verwerken van persoonsgegevens, vallen erbuiten.

ARVODI-2018: de aansprakelijkheidsverdeling

De ARVODI-2018 bevat een aantal bepalingen waarin de aansprakelijkheid bij de opdrachtnemer wordt neergelegd. Zo volgt uit artikel 21 ARVODI-2018 dat de opdrachtnemer aansprakelijk is voor schade aan gebruikte zaken die eigendom zijn van de opdrachtgever. Ook de schade die de opdrachtnemer zelf of een derde oploopt als gevolg van het gebruik van de zaken van opdrachtgever komt geheel voor rekening en risico van opdrachtnemer.

Ook verplichtingen met betrekking tot het personeel van de opdrachtnemer, komen voor de rekening van opdrachtnemer. De opdrachtnemer vrijwaart de opdrachtgever van elke aansprakelijkheid op dat punt.

ARVODI-2018: de schadevergoedingsverplichting

Ook onder de ARVODI is de hoogte van de schadevergoeding beperkt. Die is volgens artikel 21 ARVODI-2018 gerelateerd aan de hoogte van de waarde van de opdracht. Het bedrag van de vergoeding is per gebeurtenis en per jaar gelimiteerd:

- Voor opdrachten met een totale waarde tot €50.000,- is de aansprakelijkheid beperkt tot maximaal €150.000,- per gebeurtenis en €300.000,- per contractjaar;
- Voor opdrachten van €50.000,- tot €100.000,- wordt maximaal €300.000,- per gebeurtenis en €500.000,- per jaar vergoed;
- Voor opdrachten met een waarde van €100.000,- tot €150.000,- euro is dit €500.000,- en €1.000.000,-;

- Wanneer de waarde van de opdracht tussen de €150.000,- en €500.000,- ligt, is de vergoeding maximaal €1.500.000,- per gebeurtenis en €3.000.000,- per jaar;
- Voor opdrachten met een hogere waarde geldt: €3.000.000,- per gebeurtenis en €5.000.000,- per jaar.

Deze beperking vervalt echter wanneer derden letsel- of overlijdensschade hebben geleden, wanneer er sprake is van opzet of grove schuld aan de zijde van de wederpartij of diens personeel, in geval van schending van intellectuele eigendomsrechten en in geval van een tussen partijen gesloten overeenkomst betreffende de verwerking van persoonsgegevens: ten aanzien van aanspraken op schadevergoeding en door de toezichthouder opgelegde boetes.

2.2.2 Aansprakelijkheid en intellectuele eigendomsrechten
De GIBIT, ARBIT-2018 en ARVODI-2018 kennen een specifieke regeling rondom aansprakelijkheid voor schendingen van intellectuele eigendomsrechten. De aansprakelijkheid voor vorderingen van derden die voortkomen uit inbreuken op intellectuele eigendomsrechten, is volledig bij de opdrachtnemer neergelegd. De limiteringen die de aansprakelijkheidsregelingen uit de ARBIT-2018, GIBIT en de ARVODI-2018 kennen, zijn in deze gevallen niet van toepassing.

Volgens artikel 17 lid 7 van de GIBIT garandeert de opdrachtnemer dat de door hem geleverde ICT-prestaties geen inbreuk maken op intellectuele eigendomsrechten of andere rechten van derden. Hij vrijwaart de opdrachtgever van alle aanspraken van derden die daarop gebaseerd zijn. Zoals eerder is genoemd, zijn de beperkingen van de aansprakelijkheid van artikel 13 lid 2 GIBIT in dit geval niet van toepassing. Hetzelfde geldt onder de ARBIT-2018 (artikel 8.5 & 26.4) en de ARVODI-2018 (artikel 21.3.c & 24.7).

Daarnaast vrijwaart de opdrachtnemer onder artikel 8.5 van de ARBIT-2018 de opdrachtgever van alle schade en kosten waartoe opdrachtgever in een procedure mocht worden veroordeeld. Ook de kosten van de procedure zelf zullen door de opdrachtnemer betaald moeten worden.

2.3 Compliance

De auteursrechten en (eventuele) aansprakelijkheden van de contractspartijen tegenover elkaar zijn in kaart gebracht. Vervolgens moet worden geïnventariseerd in hoeverre de software compliant is aan de voorwaarden voor het gebruik van bestaande softwarecomponenten, geheimhouding en de AVG. Op basis van deze inventarisatie kan worden bepaald in hoeverre de software (al) geschikt is om als open source beschikbaar te (laten) stellen.

2.3.1 Gebruikte bestaande (software)componenten
In software zal vrijwel altijd gebruik zijn gemaakt van reeds bestaande softwarecomponenten van derden waar (OSS-)licenties op van kracht zijn. In dat geval is het van groot belang dat de overheid inzicht krijgt in de toepasselijke voorwaarden op de software.

Een simpel voorbeeld is een afvalwijzer: deze app toont de burger wanneer welk afval aan te bieden. De software van deze app kan gebruik maken van bestaande softwarecomponenten, zoals een kalender, ontworpen door een derde. Het kan zijn dat op deze kalenderfunctie een afzonderlijke (OSS-) licentie van kracht is.

De inventarisatie is van belang voor de vraag of de overheid wel of niet over zou moeten gaan tot het vrijgeven van de software. Dit is afhankelijk van welke voorwaarden de overheid en de afnemers van de vrijgegeven software moeten nakomen.

Het in kaart brengen van het (eventuele) gebruik van bestaande softwarecomponenten kan de overheid doen door informatie in te winnen bij de ontwikkelaar(s) van de software. Vervolgens moet inzicht worden verkregen onder welke voorwaarden gebruik mag worden gemaakt van deze bestaande componenten.

Onder de ARVODI-2018, ARBIT-2018 en GIBIT-2016 dient de ontwikkelaar van de software (derde) een eeuwigdurend en onherroepelijk gebruiksrecht te verlenen aan de overheid voor bestaande componenten in software.

Voor zover het om deze derdenprogrammatuur gaat, bepaalt de GIBIT vervolgens dat de licentievoorwaarden daarvan prevaleren boven de softwareontwikkelingsovereenkomst (artikel 19 lid 8 GIBIT). Ook als de GIBIT niet van toepassing is, zullen de licentievoorwaarden die betrekking hebben op de derdenprogrammatuur natuurlijk in acht moeten worden genomen, ongeacht wat de overeenkomst tussen de leverancier en de opdrachtnemer bepaalt.

Daarnaast moet de softwareontwikkelaar die derdenprogrammatuur zal gebruiken, dit in het aanbod aan de opdrachtgever mededelen. Hij moet dan ook de toepasselijke licentievoorwaarden ter beschikking stellen aan de opdrachtgever (artikel 19 GIBIT)

Het is dus afhankelijk van de licentievoorwaarden op de derdenprogrammatuur of het open sourcen van de software die deze derdenprogrammatuur bevat is toegestaan en onder welke voorwaarden. Dit is van belang voor de uiteindelijke licentiekeuze (zie §3.2).

Daarnaast maakt software vaak gebruik maken van bestaande databestanden. De toegang tot dergelijke data is dan ook van groot belang.

Teruggrijpend naar het hierboven genoemde voorbeeld van de afvalwijzer. De software van deze app heeft geen waarde als er geen toegang is tot een lijst met ophaaldata en/of -plaatsen in de gekozen gemeente. Wordt deze app als project aangeboden, dan zou dus ook de toegang tot deze lijst met gegevens gefaciliteerd worden.

2.3.2 Geheimhouding

Ook geheimhouding is een belangrijk punt van aandacht bij het open source beschikbaar stellen van software. Vertrouwelijke gegevens en zelfs de broncode

kunnen onder geheimhouding zijn gedeeld. Wanneer de auteursrechten op deze broncode overgegaan zijn op de opdrachtgever (de overheid) kan die geheimhouding mogelijk van kracht blijven.

Voor de overheid is het van belang een inschatting te maken van de impact van het ter beschikking stellen van de software ten opzichte van de vertrouwelijke informatie in de software. Dit geldt met name wanneer de software toegang biedt tot gevoelige persoonlijke gegevens of tot inlichtingen waarvan openbaarmaking het belang van de staat, de rechtspraak, de burgers of bedrijven in gevaar kan brengen.

Daarnaast moet worden nagegaan hoe binnen de relevante contracten de geheimhouding is geregeld.

2.3.3 AVG

Onder omstandigheden kan de software raken aan de Algemene Verordening Gegevensbescherming (hierna: AVG). De AVG stelt formeel geen regels aan software an sich, maar organisaties die software willen inzetten voor verwerking van persoonsgegevens krijgen daar wel mee te maken. Zo stelt de AVG bijvoorbeeld "privacy by design" en "privacy by default" verplicht.

Privacy by design houdt in dat de voor verwerking gebruikte mechanismen zo zijn ontworpen dat zij zoveel mogelijk rekening houden met de privacy van betrokkenen en de vereisten uit de AVG. Een softwaresysteem dat hieraan voldoet, zou dus bijvoorbeeld functionaliteiten ingebouwd moeten hebben waarmee betrokken inzage (artikel 15 AVG) in hun persoonsgegevens kunnen krijgen. Andere functionaliteiten die in dit kader relevant zijn, zijn bijvoorbeeld gericht op het minimaliseren van de hoeveelheid persoonsgegevens (geen onnodige velden gebruiken) en het zo spoedig kunnen mogelijk pseudonimiseren van persoonsgegevens.

Privacy by default houdt in dat de standaardinstellingen bij de verwerking van persoonsgegevens zo zijn gekozen dat de privacy maximaal wordt geborgd. Bij een softwaresysteem houdt dit bijvoorbeeld in dat alle opties binnen het systeem voor het delen van persoonsgegevens standaard uit staan en dat gebruikers van het systeem actief moeten handelen om de persoonsgegevens wel te kunnen delen, wanneer zij dit wensen.

De mate van compliance van de software aan de AVG is dan ook van belang bij de afweging of een specifiek softwareproduct nog moet worden aangepast alvorens tot de beschikbaarstelling van de broncode wordt overgegaan.

3 Keuzes ten aanzien van governance

In hoofdstuk 1 en 2 zijn verschillende handvatten gegeven aan de overheid bij het maken van inventarisaties en afwegingen ten opzichte van de bestuurlijke keuzes en keuzes ten aanzien van een specifiek product. Op basis daarvan heeft de overheid inzicht in de randvoorwaarden voor de keuze of zij de broncode wel of niet als open source gaat vrijgeven, of dat de broncode eerst op onderdelen aangepast moet worden. De volgende stap is het maken van keuzes ten aanzien van de governance van het project.

3.1 Governance van het project

Software aan het publiek beschikbaar stellen is geen kwestie van eenmalig de broncode bestanden op een website of repository plaatsen.
Het beschikbaar stellen van open source software is een proces dat moet worden begeleid door een inhoudelijk betrokken medewerker. Deze stimuleert het project en laat het tot bloei komen door derden erbij te betrekken. De rol van deze derden wordt dan langzaam maar zeker groter, totdat op zeker moment de eigen medewerker terug kan treden en het project zelfstandig kan opereren.

Keuzes ten aanzien van governance kunnen alleen worden gemaakt wanneer wordt nagedacht over hoe om te gaan met de beschikbaarstelling van de software. Daarbij kan worden gedacht aan de wijze van beschikbaarstelling, doorontwikkeling, de licentiekeuze en de plaats van beschikbaar stellen. Hieronder worden een aantal handvatten gegeven om een weloverwogen beslissing te maken ten aanzien van de governance van het project.

3.1.1 Wijze van beschikbaarstelling

Onder governance moet onder andere worden verstaan het maken van keuzes ten aanzien van de beschikbaarstelling. Wat betreft de wijze van beschikbaarstelling is de meest simpele vorm dat de broncode op een website wordt gepubliceerd, waarna de nodige bekendheid wordt gegenereerd om deze onder de aandacht van relevante partijen te brengen. Dit kan een eigen website zijn, maar ook een site van een derde. Hierop wordt nader ingegaan in §3.3.

Ook is het mogelijk om de leverancier te vragen of hij de broncode wil publiceren, en in voorkomende gevallen wil inbrengen bij een al bestaande open source community.

Bij grotere projecten is het soms wenselijk om de governance in een eigen stichting onder te brengen. Met deze private rechtspersoon kan een (door overheidsdeelnemers te benoemen) bestuur de doorontwikkeling van het specifieke product op zich nemen, de intellectuele eigendomsrechten beheren en eventueel fondsen werven die ten behoeve van het project kunnen worden ingezet. De lange termijn continuïteit van het project wordt hiermee geborgd. Ook kan gekozen worden voor constructies zoals de Commons Conservancy.[4] Dat is een Nederlandse stichting die speciaal voor dit doel is opgericht, en waarbij projecten zich kunnen aansluiten.

[4] Commonsconservancy.org

3.1.2 Doorontwikkeling

Vervolgens moet een keuze worden gemaakt ten aanzien van de beoogde bemoeienis bij de doorontwikkeling van de software.

Er kan enerzijds voor gekozen worden de software in een community op een website te (laten) plaatsen, zonder enige actieve bemoeienis bij de doorontwikkeling van de software. Zo kunnen anderen naar eigen inzicht verder werken aan de software. In dat geval heeft de overheid geen controle meer over wat anderen met de software doen en welke doorontwikkelingen er plaatsvinden. Afhankelijk van de activiteit binnen de community kan dat prima uitpakken, maar wel is het van belang op te merken dat dergelijk "over de schutting gooien" niet het gewenste resultaat heeft wanneer de software nog niet "volwassen" is, door bijvoorbeeld het ontbreken van functionaliteiten.

Anderzijds is het mogelijk voor de overheid om actieve bemoeienis te houden bij verdere ontwikkelingen, al dan niet door tussenkomst van een leverancier. Zo kan de overheid bijvoorbeeld bepalen dat zij actief betrokken wil zijn bij de doorontwikkeling van de software door middel van het wel/niet accepteren van door de community als Pull Request voorgestelde aanpassingen aan de broncode.

Bij de keuze ten aanzien van doorontwikkeling is het belangrijk om stil te staan bij de aansprakelijkheidsaspecten die hier een rol spelen. Hoe meer de overheid zich actief bemoeit met de doorontwikkeling, hoe meer aansprakelijkheidsrisico's zich kunnen voordoen. Op de aansprakelijkheid jegens derde partijen wordt in §3.2.5 nader ingegaan.

Daarnaast het is belangrijk om na te gaan welke garanties (al dan niet tegen betaling) de overheid wil bieden ten aanzien van de doorontwikkelde versie van de software. Het aanbieden van extra garanties door overheden ten aanzien van de software valt buiten de scope van deze handreiking. Indien overheden dergelijke extra garanties willen bieden, wordt het aangeraden om maatwerkadvies in te winnen. Het tegen betaling bieden van extra garanties heeft namelijk mogelijk gevolgen voor de aansprakelijkheid en kan bovendien een marktverstorende werking hebben.

3.2 Licentiekeuze

Wanneer de keuze tot beschikbaarstelling is gemaakt; ten aanzien van een specifiek product de eigendomsrechten en aansprakelijkheid zijn geborgd; de broncode is getoetst op compliance; de keuzes ten aanzien van de governance zijn gemaakt, dan kan de software auteursrechtelijk als open source worden vrijgegeven. Dit vereist een licentiekeuze. De licentie houdt de toestemming in tot gebruik en verspreiding van de software, in combinatie met de voorwaarden waaronder die toestemming wordt gegeven. Deze licentiekeuze is afhankelijk van de inventarisaties, afwegingen en keuzes die hiervoor zijn gemaakt.

3.2.1 Software-licenties
Grofweg zijn drie verschillende soorten licenties te onderscheiden:

1. Een beperkte licentie, die alleen het gebruik toestaat.
2. Een brede licentie, die ook aanpassen en door ontwikkelen toestaat.
3. Een gestandaardiseerde open source licentie.

Optie 1 is eigenlijk alleen geschikt wanneer het overheidsorgaan grip wil houden op de software. Partijen die de software willen aanpassen of verder verspreiden, zullen dan immers apart toestemming moeten vragen. Dit is meestal niet wenselijk vanwege de *overhead* die dit met zich meebrengt en het risico op ongelijk behandelen van marktpartijen.

Met optie 2 worden de nadelen van optie 1 opgeheven, maar kan men toch eigen criteria of randvoorwaarden stellen. In beginsel is de keuze vrij in wat wel en niet toe te staan en welke randvoorwaarden te stellen. Een nadeel van deze optie is dat de licentietekst opgesteld moet worden en dat potentiële afnemers deze moeten evalueren op juridische acceptatiecriteria. Dit kost tijd en zeker bij kleinere marktpartijen/consumenten heeft men dat er vaak niet voor over.

De keuze voor optie 3 (open source) is vaak het alternatief wanneer een eigen licentie niet op de gewenste wijze opgesteld kan worden. Open source licenties zijn algemeen bekend in de markt, zodat men kan volstaan met enkel de naam van de te kiezen licentie te noemen. Deze licenties zijn ook sterk beschermend voor de leverancier van de software (in dit geval de overheid); de licenties beperken alle verplichtingen en aansprakelijkheden maximaal.

Bij de keuze voor open source gelden drie smaken:

1. *Academic* open source: verplichte naamsvermelding van de auteur(s), verder volledige vrijheid voor de afnemer, geen verplichtingen en geen aansprakelijkheid voor de leverancier.
2. *Weak copyleft:* de afnemer moet wijzigingen aan de software ook als open source beschikbaar stellen, maar mag eigen aanvullende software naar eigen inzicht uitbrengen. Er zijn geen verplichtingen en geen aansprakelijkheid voor de leverancier.
3. *Strong* copyleft: de afnemer moet naast wijzigingen ook eigen aanvullende software als open source beschikbaar stellen. Er zijn geen verplichtingen en geen aansprakelijkheid voor de leverancier.

De keuze voor de gewenste open source licentie hangt dus af van de mate van 'copyleft', oftewel de verplichting tot delen die men de afnemers van de software wil opleggen. De keuze voor strong copyleft levert in de praktijk vele bijdragen op van enthousiaste kleine partijen, maar laat grote organisaties vaak huiveriger staan tegenover de software. De keuze voor *academic* open source geeft vaak het omgekeerde.

In §3.2.2 worden verschillende standaard open source licenties uit de praktijk toegelicht waar de overheid uit zou kunnen kiezen bij haar licentiekeuze.

3.2.2 Standaard open source licenties

Voor het open sourcen van software is het van belang dat een weloverwogen keuze wordt gemaakt ten aanzien van de licentievoorwaarden waaronder de software wordt vrijgegeven. Voor het maken van een weloverwogen keuze is het belangrijk goed in kaart te brengen welke voorwaarden de overheid wil stellen aan het gebruik en verspreiding van de software en welke standaard open source licentie hier het beste op aansluit.

> *Zo kunnen open source licentievoorwaarden de afnemer bijvoorbeeld verplichten om de naam van de auteur te vermelden als de afnemer de open source software opneemt in een product. Ook kan in de voorwaarden staan dat de broncode van de software meegeleverd moet worden. Tevens kan het verplicht zijn om aanpassingen bij te houden of aangepaste versies een andere naam te geven.*

In de praktijk zijn de meest gebruikte licenties de BSD licentie, de Mozilla Public License (MPL), de GNU Library of Lesser General Public License (LGPL), de GNU General Public License (GPL) en de European Union Public Licence (EUPL).

BSD licentie

De BSD licentie is een voorbeeld van *academic* open source. De licentie is kort en vrij eenvoudig. De enige voorwaarde die wordt gesteld is dat afnemers van de software de naam van de auteur(s) moeten vermelden als ze de software in hun eigen producten verwerken, en dat geheel weer onder een andere licentie willen verspreiden. Verder is het gebruik en alle vormen van verder verspreiden toegestaan, inclusief het door een afnemer tegen betaling verder verspreiden van enkel de objectcode.

Deze licentie is geschikt voor het open sourcen van software, indien de overheid graag wil dat veel mensen gebruik maken van de software en de overheid commercieel hergebruik van de software toestaat. Eventuele door derden aangebrachte verbeteringen komen dan echter niet per definitie gratis ter beschikking.

Mozilla Public License (MPL)

Een voorbeeld van een *weak copyleft* licentie is de MPL. Voor verspreiding van de broncode geldt (in tegenstelling tot de objectcode) dat dit enkel en alleen mag gebeuren onder de MPL licentie. Ook wijzigingen in de broncode (een "derived work") moeten onder de MPL openbaar worden gemaakt op het moment dat de

(gewijzigde) software beschikbaar komt voor derden. In de broncode moet tevens een vastgestelde “copyright notice” worden opgenomen met een verwijzing naar de oorspronkelijke auteur(s).

Bij een verspreiding van de code in objectcode vorm is de verspreider verplicht om een voor de eindgebruiker leesbaar bericht in de executable en de documentatie op te nemen waarin staat dat de broncode van de MPL module beschikbaar is onder de condities van de MPL. Ook moet het daarbij aangeven hoe de verspreider heeft voldaan aan zijn eventuele verplichtingen om de broncode van de MPL software beschikbaar te stellen of te houden.
Indien MPL software verspreidt wordt in object code vorm onder een andere “zelf gekozen licentie”, dan mag deze licentie geen beperkingen opwerpen ten aanzien van de rechten welke een eindgebruiker heeft op de broncode volgens de voorwaarden van de MPL. Tevens moet overduidelijk worden aangegeven dat eventuele garanties alleen worden aangeboden door de verspreider, en niet door de auteurs en bewerkers van de MPL software.

GNU Library of Lesser General Public License (LGPL)
Nog een voorbeeld van een *weak copyleft* licentie is de LGPL. Het is uitsluitend gericht op zogeheten softwarelibraries. Software waarin gebruik wordt gemaakt van dergelijke softwarelibraries hoeft zelf niet onder de LGPL te worden vrijgegeven. Wel moeten onder de LGPL de aangebrachte wijzigingen in de broncode van de libraries weer open source ter beschikking worden gesteld.

GNU General Public License (GPL)
Een voorbeeld van een *strong copyleft* licentie is de GPL. Onder de GPL uitgegeven software mag je gebruiken en verspreiden (zowel commercieel als niet-commercieel), mits je dat recht (zonder restricties) doorgeeft aan anderen. Daarnaast moeten de auteur(s) van de software worden vermeld. Dit komt erop neer dat wanneer een afnemer de software wil verspreiden, de afnemer de broncode bij zal moeten voegen. Deze broncode moet weer verder worden verspreid onder de GPL.

De bedoeling achter de GPL is dat mensen die software onder de GPL willen gebruiken, ook de broncode moeten aanbieden wanneer zij de gewijzigde versie verspreiden. Hiermee kan de maatschappij weer profiteren van de wijzigingen van de software die ter beschikking komen.

European Union Public Licence (EUPL)
De EUPL is de Europese overheidsvariant van een copyleft licentie. De nadruk in de EUPL ligt op het voldoen aan lokale wetgeving in EU-landen en de mogelijkheden tot integratie met softwarecomponenten onder andere open source softwarelicenties, zoals de GPL. Een opvallend kenmerk is dat de EUPL beschikbaar is in alle officiële talen van de Europese Unie en bovendien gebaseerd is op Europese wetgeving. Dit is tegensteling tot de meeste andere open source licenties die doorgaans een Amerikaanse structuur kennen. De EUPL verplicht de distributeur van software om de broncode altijd mee te leveren, of deze op een vrij toegankelijke plaats aan te bieden.

3.2.3 Zelf een licentie opstellen

Het is mogelijk om zelf een licentie op te stellen. Echter, hierbij moet worden gewezen op de (juridische) valkuilen die zich daarbij voordoen. Het is namelijk lastig om alle mogelijke situaties te voorzien waarin anderen software willen gaan gebruiken en/of verspreiden. Daarnaast doen zich ook risico's voor bij het juridisch juist vastleggen van de rechten en plichten van gebruikers. Het is dan ook sterk aan te bevelen gebruik te maken van een standaardlicentie die het beste bij de belangen van het project aansluit.

3.2.4 Licentiekeuze en derdenprogrammatuur

In §2.3.1 is reeds aangegeven dat de overheid rekening dient te houden met de licentievoorwaarden van gebruikte bestaande softwarecomponenten in de software. Deze licentievoorwaarden kunnen invloed hebben op de te maken licentiekeuze. Het kan namelijk zo zijn dat de toepasselijke licentie voorwaarden stelt aan het gebruik en verdere verspreiding van de gebruikte componenten.

> *Ter illustratie: software bevat reeds bestaande softwarecomponenten waar de GPL op van toepassing is. Wanneer deze software open source ter beschikking wordt gesteld moet hier rekening mee gehouden worden. De GPL verplicht namelijk onder andere dat wijzigingen in de software ook openbaar moeten worden gemaakt onder de GPL.*

3.2.5 Licentiekeuze en aansprakelijkheid jegens derden

Ook de wens om aansprakelijkheid uit te sluiten kan invloed hebben op de licentiekeuze. Software kan fouten bevatten die volgens de wet kunnen leiden tot aansprakelijkheid jegens derden. Het kan dan gaan om programmeerfouten, ontwerpfouten of andere fouten. Aansprakelijkheid voor fouten is in beginsel vrij te beperken in de licentieovereenkomst. Dit is zeker rechtsgeldig wanneer het overheidsorgaan volstaat met het beschikbaar stellen van de software.

<u>Wettelijke aansprakelijkheid</u>

Om de grondslag voor aansprakelijkheid te bepalen is het van belang door wie de software is ontwikkeld. Indien de ontwikkelaar een werknemer is van de overheid, zal de grondslag voor aansprakelijkheid in artikel 6:170 BW zijn gelegen. Als het om een zelfstandige gaat die bijvoorbeeld onder een overeenkomst van opdracht werkt, zal artikel 6:171 BW de grondslag kunnen bieden.

Omdat de opdrachtgever en opdrachtnemer op grond van artikel 6:171 BW beide aansprakelijk zijn voor schade ontstaan door fouten van de opdrachtnemer, kunnen derden in beginsel kiezen wie ze aanspreken als deze aansprakelijkheidsgrondslag van toepassing is. In de ARBIT-2018, GIBIT en ARVODI-2018 zijn afspraken gemaakt die tussen de contractspartijen regelen wie de schade draagt. De partijen kunnen elkaar op grond van hun contractuele verhouding aanspreken voor schade van derden. De opdrachtnemer is dan ook verplicht verzekerd tot een bepaald bedrag.

De verschillende grondslagen voor aansprakelijkheid worden hieronder kort uiteengezet.

Ondergeschikte hulppersonen (6:170 BW)
Artikel 6:170 BW biedt een grondslag voor kwalitatieve aansprakelijkheid van werkgevers voor fouten van ondergeschikte hulppersonen. Wanneer de software door een werknemer of anderszins ondergeschikte van de overheid wordt ontwikkeld, is deze aansprakelijkheidsgrondslag relevant.

Voor aansprakelijkheid is vereist dat de ondergeschikte een fout heeft gemaakt terwijl hij in dienst van de werkgever een taak vervulde, indien de kans op de fout door de opdracht tot het verrichten van deze taak is vergroot. Degene in wiens dienst de werknemer de taak verricht heeft, moet zeggenschap kunnen hebben over de gedraging waarin de fout zich heeft voorgedaan. Kortom, de overheid moet een instructiebevoegdheid hebben gehad. Het vereiste van een dienstbetrekking houdt niet in dat deze een structureel karakter moet hebben, het kan ook gaan om een incidentele dienstbetrekking. Wel is het zo dat een overeenkomst van opdracht doorgaans niet onder deze aansprakelijkheidsgrond zal vallen.

Op grond van artikel 6:170 BW zijn zowel de werkgever als de werknemer jegens de derde aansprakelijk. Volgens lid 3 heeft de werknemer dan een verhaalsrecht op de werkgever. De werkgever dient de schade te dragen, tenzij die schade het gevolg is van opzet of bewuste roekeloosheid van de werknemer. Hiervan mag bij schriftelijke overeenkomst worden afgeweken, maar niet verder dan het bedrag waarvoor de werknemer zelf is verzekerd.

Niet-ondergeschikte hulppersonen (6:171 BW)
Meestal zal er echter sprake zijn van een overeenkomst van opdracht waarmee een zelfstandige hulppersoon wordt ingeschakeld om de software te ontwikkelen. In dat geval moeten we de aansprakelijkheidsgrondslag zoeken in artikel 6:171 BW. Dit artikel regelt de aansprakelijkheid van opdrachtgevers voor fouten van hun opdrachtnemers.

In dit kader is vereist dat er een opdrachtrelatie bestaat tussen de opdrachtgever en de zelfstandige en dat deze zelfstandige of diens personeel een fout heeft gemaakt. De werkzaamheden van de opdrachtnemer moeten verder zijn uitgeoefend ter uitoefening van het bedrijf van de opdrachtgever. Dit houdt niet in dat de opdrachtgever een winstoogmerk moet hebben, waardoor het artikel ook op overheden van toepassing kan zijn. Echter, indien het gaat om het uitvoeren van een publieke taak, is niet aan dit criterium voldaan en is de overheid als opdrachtgever niet aansprakelijk voor de fout van de opdrachtnemer.

Eigen onrechtmatig handelen (6:162 BW)
De algemene grondslag van de onrechtmatige daad kan dienen als 'vangnetbepaling' als de hierboven genoemde grondslagen niet aan de orde zijn. Dan is wel vereist dat de overheid zelf onrechtmatig heeft gehandeld door de software open source beschikbaar te stellen. Artikel 6:162 kan zodoende een rol spelen.

> *Dit is bijvoorbeeld het geval wanneer de software een gebrek heeft, waar de overheid zich bewust van was, maar zij de software toch zonder waarschuwing open source ter beschikking heeft gesteld, met schade tot gevolg.*

Productaansprakelijkheid
Volgens artikel 6:185 lid 1 BW is een producent aansprakelijk voor gebreken in het product. Software als zodanig valt over het algemeen niet onder het begrip 'product' in de zin van deze regeling. Daarentegen is software wel aan te merken als 'product' in de zin van Richtlijn 85/374/EEG, wanneer de software op een materiële gegevensdrager is gevestigd.

Aansprakelijkheid voor het verwerken van persoonsgegevens
Het is denkbaar dat de ontwikkelde software kan worden gebruikt voor het verwerken van persoonsgegevens, wat aanleiding kan geven tot schadeclaims. De verwerkingsverantwoordelijke en verwerker zijn aansprakelijk voor de schade die een derde heeft geleden als gevolg van een verwerking in strijd met de AVG (artikel 82 lid 1 AVG). Echter, wanneer derden de open source ter beschikking gestelde software gebruiken om persoonsgegevens te verwerken, dan is de overheid geen verwerker en geen verwerkingsverantwoordelijke. In dat geval is de overheid niet aansprakelijk voor eventuele ontstane schade.

Daarentegen kan de overheid wel aansprakelijk worden gehouden door derden voor problemen in de software waardoor een datalek ontstaat. Als het probleem het gevolg is van een fout van de ontwikkelaar, kan de overheid de schade op de ontwikkelaar verhalen volgens de contractuele afspraken die tussen hen gelden. Dit is in §2.2 aan de orde gekomen.

Risico's
Vervolgens is het van belang aandacht te besteden aan de risico's en hoe met deze risico's om te gaan. Daarbij wordt als uitgangspunt genomen dat overheden het liefst zo weinig mogelijk risico nemen.

De aansprakelijkheidsbepalingen uit de ARBIT-2018, GIBIT en ARVODI-2018 die in §2.2 zijn besproken, bieden geen bescherming tegen aansprakelijkheid als zodanig. Ze regelen slechts de onderlinge verhouding tussen de contractspartijen en zorgen zo voor onderlinge verhaalsrechten, in plaats van aansprakelijkheidsuitsluitingen jegens derden.

Derden kunnen in beginsel beide partijen aansprakelijk stellen en zich op beide partijen verhalen. De contractspartijen moeten hun verhaal op elkaar onderling regelen. Indien de opdrachtnemer weinig financiële middelen heeft levert dit alsnog geen problemen op, omdat de opdrachtnemer verplicht is zich te verzekeren tot een bepaald bedrag. Echter, faillissement van de opdrachtnemer kan wel problematisch zijn voor opdrachtgever.

Uitsluiting van aansprakelijkheid
Om zoveel mogelijk risico's te voorkomen, is het belangrijk voor de overheid om de aansprakelijkheid tegenover derden uit te sluiten in de open source softwarelicentie. Uitgangspunt is dat de overheid niet aansprakelijk is ten aanzien van de open source vrijgegeven software. Hierbij moet wel worden opgemerkt dat het niet mogelijk is om aansprakelijkheid uit te sluiten voor opzet of grove schuld.

Wel moet bij het gebruiken van een exoneratiebeding in licentievoorwaarden rekening worden gehouden met het feit dat licentievoorwaarden worden aangemerkt als algemene voorwaarden in de zin van artikel 6:231 BW. Indien de licentienemer een consument of kleine onderneming is, kunnen zij een beroep doen

op de grijze en zwarte lijst. Op grond van artikel 6:233 sub a BW en 6:237 sub f BW wordt een exoneratiebeding namelijk vermoed onredelijk bezwarend te zijn. In dat geval is het exoneratiebeding vernietigbaar, tenzij de licentiegever (de overheid) kan aantonen dat het beding niet onredelijk is.

Het is aan te raden een exoneratiebeding op te nemen in de licentievoorwaarden. Hiervoor is het dus van belang dat de overheid kan aantonen dat het beding niet onredelijk bezwarend is. Mogelijke argumenten om aan te tonen dat het beding niet onredelijk bezwarend is kunnen zijn dat de software gratis ter beschikking is gesteld. Daarnaast weet de overheid niet wie de software gaat gebruiken. De overheid heeft dan ook niet kunnen overleggen over de doeleinden van het gebruik van de software met gebruikers. Dit maakt ook dat de overheid extra zorgvuldigheid mag verwachten van de gebruiker. Tevens maakt de openheid van de broncode het mogelijk voor de gebruiker om de software volledig te onderwerpen aan een validatieonderzoek of broncodeanalyse. Fouten in de software kunnen sneller worden ontdekt, nu de software en broncode zijn blootgesteld aan medeontwikkelaars die iedere nieuwe release kunnen uittesten.

Naast de mogelijkheid om het vermoeden van onredelijkheid van het exoneratiebeding te weerleggen, kan de overheid terugvallen op de contractuele verhouding met de ontwikkelaar van de software. De verhaalsrechten en aansprakelijkheden die tussen de beide contractspartijen gelden, zijn te vinden in §2.2.

Zoals hierboven in §3.1.1 is aangegeven, moet de software ergens beschikbaar worden gesteld. Enkel de broncode als download aanbieden, is niet genoeg. De maatschappij verwacht vandaag de dag dat er faciliteiten zijn voor centraal beheer van aanpassingen en uitbreidingen.
In dat geval is de beste praktijk om de broncode onder te (laten) brengen bij een zogeheten broncodeplatform (source code repository), vanaf waar derden de software eenvoudig kunnen beheren, bijdragen kunnen toevoegen of alternatieve versies ontwikkelen. Hiervoor zijn een aantal bekende platformen beschikbaar. Niet limitatief valt daarbij te denken aan:

- *Github* (www.github.com): Dit platform is verreweg de grootste partij als het gaat om publiek beschikbaar stellen van broncode en faciliteren van het aanpassen en uitbreiden daarvan.
- *BitBucket* (www.bitbucket.com): Dit platform wordt vaak gebruikt bij softwarepakketten gericht op grotere ondernemingen (enterprise).
- *SourceForge* (www.sourceforge.com): Dit project is al wat ouder en richt zich met name op open source software gericht op de Linux omgeving.
- *JoinUp/OSOR* (https://joinup.ec.europa.eu/solutions)
  Deze Europese dienst wordt veel gebruikt door overheden om broncodes aan te bieden.

Het is ook mogelijk een eigen platform op te zetten waar de broncode beschikbaar wordt gesteld. Het opzetten en onderhouden van een eigen platform vereist echter veel investeringen. Niet alleen kost het opzetten van een eigen platform tijd en geld, ook het beheren van het platform en de promotie daarvan kunnen duur en tijdrovend zijn. Wanneer de overheid aanhaakt bij bestaande platforms, kunnen anderen de software ontdekken, zonder te moeten investeren in het beheren en promotie van een platform.

De hierboven genoemde marktpartijen zijn (met uitzondering van het OSOR-platform) private partijen waarmee formeel een overeenkomst wordt aangegaan, zij het dat deze vaak gratis wordt aangegaan. Deze overeenkomst is in beginsel niet onderhandelbaar. Men gaat als afnemer akkoord met de online aangeboden voorwaarden, ook als overheid. Eigen inkoopvoorwaarden kunnen niet van toepassing worden verklaard. In sommige gevallen moet wel worden betaald voor de dienstverlening. De bedragen zijn gewoonlijk dusdanig klein dat deze dienstverlening niet aanbesteed hoeft te worden.

Conclusie

Om over te kunnen gaan op het als open source beschikbaar stellen van software dient de overheid allereerst te onderzoeken of de software samenhangt met, en dienstbaar is aan de publieke taak. Daarbij moet gekeken worden naar het aard en het doel van de activiteiten en de regels waaraan zij zijn onderworpen. Is van dat laatste sprake, dan is de Wet Markt en Overheid niet van toepassing.
Mocht deze samenhang danwel de dienstbaarheid aan de publieke taak niet direct aantoonbaar zijn, dan kan er -indien de software door een marktpartij wordt ontwikkeld- voor gekozen worden om deze leverancier toe te staan de software zelf als open source beschikbaar te stellen.
Mochten deze twee situaties beide niet toepasbaar zijn, dan kan er tot slot nog worden onderzocht of er voor het beschikbaar stellen van de software een Algemeen Belang besluit moet worden genomen. Met een dergelijk besluit kan de overheid ervoor zorgen dat de Wet Markt en Overheid niet van toepassing is op het ter beschikking stellen van die software.

Auteursrecht
Het door de overheid vrijgeven van software is mogelijk wanneer de overheid zelf auteursrechthebbende is of wanneer alle auteursrechthebbenden van de software daarvoor hun toestemming verlenen. Daarnaast moet rekening worden gehouden met persoonlijkheidsrechten van de maker van de software. Consequentie kan zijn dat auteursrechthebbende(n)/de maker(s) achteraf een schadeclaim indienen en/of het project bij de rechter van de markt laten halen. Alleen al de dreiging van een dergelijke juridische actie kan genoeg zijn een project te laten sneuvelen. Dit maakt dat het van groot belang dat de auteursrechten op software vooraf in kaart worden gebracht en (contractueel) goed zijn geregeld. Als alternatief kan ervoor worden gekozen om een leverancier toe te staan zelf de ontwikkelde software beschikbaar te stellen op een openbare repository.

Aansprakelijkheid
Het is van belang om een goede inventarisatie te maken van de rechtspositie tussen de overheid en de ontwikkelaar van de software. De onderlinge afspraken over de aansprakelijkheid moeten goed geregeld zijn in het contract met de ontwikkelaar(s). Zowel in (eventuele) toepasselijke voorwaarden sets als in de afzonderlijke afspraken uit de overeenkomst met de ontwikkelaar.

Compliance
Bij het toetsen van de compliance worden verschillende inventarisaties en afwegingen gedaan op verschillende rechtsgebieden. Wanneer uit deze inventarisaties en afwegingen blijkt dat het specifieke softwareproduct nog niet compliant is aan wet- en regelgeving of contractuele (licentie)afspraken, dan moet vervolgens de belangenafweging worden gemaakt in hoeverre het verstandig is om zonder aanpassingen of voorbehouden over te gaan op het open source publiceren van de software.

Mogelijke conclusies kunnen zijn:
- Niet open source publiceren van de software;
- Risico's inperken door middel van het aanpassen van de software;
- Wel open source (laten) vrijgeven van de software.

Governance en licentiekeuze

Waar het gaat om de governance van het project is het van belang om een weloverwogen keuze te maken ten aanzien van de wijze van beschikbaarstelling en de mate van betrokkenheid bij de doorontwikkeling van de software. Deze keuzes zijn van belang voor de licentiekeuze en voor de plaats van beschikbaar stellen.
Uitgangspunt is in beide gevallen dat de overheid zo weinig mogelijk risico's loopt bij het open source beschikbaar stellen van de software. Hier dient vooral bij de licentiekeuze rekening mee te worden gehouden. Dit kan onder andere door het kiezen van standaard open source licentievoorwaarden. Voor de keuze tussen de verschillende standaard open source licentievoorwaarden is de afweging in de copyleft-sfeer van belang, met als centrale vraag: In hoeverre moeten wijzigingen van de software ook weer open source beschikbaar worden gesteld?
Het ligt voor de hand om de software beschikbaar te (laten) stellen op een reeds bekend broncodeplatform. Er moet rekening worden gehouden met de inventarisaties en afwegingen die hiervoor zijn gemaakt welk platform het beste aansluit bij de verwachtingen en behoeftes van de overheid.

Wanneer de overheid er bijvoorbeeld voor kiest om de software specifiek onder de aandacht te brengen bij andere overheden, zal een goede optie het broncodeplatform JoinUp/OSOR zijn.[5] Deze door de Europese Unie aangeboden dienst wordt namelijk veel gebruikt door overheden om software aan te bieden. Veel software wordt daar onder de EUPL aangeboden. In het geval de overheid besluit om de software aan iedereen vrij te geven en een breder groep van (private) ontwikkelaars te betrekken bij de doorontwikkeling, dan zullen andere platformen mogelijk een betere keuze zijn. Ook in dat geval kan er vanuit JoinUp/OSOR naar dat andere platform gelinkt worden. Dat is ook handig indien ervoor wordt gekozen om de leverancier zelf de broncode beschikbaar te laten stellen.

[5] https://joinup.ec.europa.eu/solutions

Opdrachtgever: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
December 2019.