

Ministerie van Volksgezondheid,
Welzijn en Sport

Wettelijke kaders rond open source

Maurice Hendriks
In samenwerking met alle bijdragers

Gepubliceerd op 10 november 2026

Creative Commons Naamsvermelding 4.0 Internationaal

Inhoud

Nationaal **2**
Wet open overheid 2
Auteurswet en Wet Markt & Overheid 3
Archiefwet 6

Europees **7**
De Verordening Cyberweerbaarheid / Cyber Resilience Act (CRA) 7

Bijdragers **8**

Nationaal

Wet open overheid

Gedeeltelijke publicatie

Er zijn verschillende redenen waarom een (open source) softwareproject niet volledig (open source) gepubliceerd kan worden:

- Er is een absolute en/of relatieve uitzonderingsgrond van toepassing vanuit de Wet open overheid.
- Een open source publicatie kan worden gezien als een economische activiteit onder de Wet markt en overheid.
- Niet alle IE-rechten zijn in bezit van degene die wil publiceren.
- Delen van de broncode bevatten vertrouwelijke informatie.

Welke belemmering er ook is, publiceer altijd de onderdelen die wel open source gepubliceerd kunnen worden. Vertrouwelijke informatie kan zwartgelakt ('zwartlakken') worden, of de belemmering kan worden weggenomen.

Let op: een beroep op vertrouwelijkheid kan niet zomaar worden gedaan. Vertrouwelijkheid geldt nooit automatisch voor het hele project. Een claim op vertrouwelijkheid moet altijd gerelateerd zijn aan een van de uitzonderingsgronden in de Woo en goed worden gemotiveerd. Wees daarnaast transparant over welke uitzonderingsgronden zijn toegepast bij het niet volledig publiceren van de broncode.

Absolute en relatieve uitzonderingsgrond

Soms hoeft de overheid informatie niet openbaar te maken. Voor bepaalde informatie bestaan uitzonderingsgronden. Denk bijvoorbeeld aan informatie die de veiligheid van de Staat in gevaar kan brengen. Deze uitzonderingsgronden zijn er in twee vormen:

Absolute uitzonderingsgronden (Woo, art. 5.1, eerste lid)

Bij deze gronden vindt geen belangenafweging plaats. Als overheidsinformatie een van de onderstaande gronden raakt, mag deze in geen geval worden gepubliceerd naar aanleiding van een Woo-verzoek:

- Eenheid van de Kroon

- Veiligheid van de Staat
- Vertrouwelijk meegedeelde bedrijfs- en fabricagegegevens
- Persoonsgegevens
- Nummers ter identificatie

Relatieve uitzonderingsgronden (Woo, art. 5.1 tweede lid)

Hier is wél een afweging van belangen nodig, bij voorkeur samen met juristen. Het publiceren van bepaalde informatie kan bijvoorbeeld marktverstorend werken. Voorbeelden van belangen die hierbij een rol kunnen spelen zijn:

- Bedrijfs- en fabricagegegevens
- Economische en financiële belangen van de overheid
- Goed functioneren van overheidsorganen

Als er uitzonderingsgronden van toepassing zijn, betekent dit niet dat er niets gepubliceerd mag worden. Alleen de onderdelen die onder de uitzondering vallen mogen zwartgelakt worden of buiten de publicatie blijven. Zorg dat in de documentatie duidelijk staat welke delen zwartgelakt zijn of niet gepubliceerd, en waarom. Beschrijf ook de functie van die onderdelen, zodat derden de functionaliteit in de lokale context kunnen begrijpen en eventueel zelf invullen.

Auteurswet en Wet Markt & Overheid

Vanuit de Wet open overheid (Woo) geldt er een inspanningsverplichting om broncode proactief openbaar te maken. De Wet hergebruik overheidsinformatie (Who) schrijft daar bovenop voor dat openbaar gemaakte broncode ook zoveel mogelijk geschikt moet worden gepubliceerd voor hergebruik. De open source licentie wordt erin aangewezen als hét instrument om dat hergebruik te bereiken.

Transparantie: ja, hergebruik: nee

Er kunnen omstandigheden zijn waarin broncode wél openbaar wordt gemaakt voor transparantiedoeleinden, maar niet voor hergebruik. Dit kan zich voordoen wanneer openbaarmaking voor hergebruik de economische belangen van de overheid zou schaden. In dat geval is sprake van een relatieve uitzonderingsgrond als bedoeld in artikel 5.1, tweede lid, van de Woo.

In zulke situaties kan broncode worden gepubliceerd zonder open-sourcelicentie, met de vermelding dat alle rechten zijn voorbehouden. De code is dan wel inzichtelijk, maar mag niet worden hergebruikt. Het opnemen van dit voorbehoud is essentieel, omdat volgens artikel 15b Auteurswet openbaar gemaakte werken van de overheid, zonder expliciet voorbehoud, vrij gebruikt en gekopieerd mogen worden door derden. De overheid behoudt altijd het auteursrecht, maar zonder voorbehoud kan dit recht niet effectief worden gehandhaafd. Door "Alle rechten voorbehouden" te vermelden, wordt hergebruik zonder toestemming uitgesloten. Neem deze vermelding idealiter ook in alle broncodebestanden op, samen met een copyrightvermelding. Bijv:

```
/*
  Alle rechten voorbehouden
  Copyright Ministerie van Volksgezondheid, Welzijn en Sport
*/
```

Wie bezit de IE-rechten?

Vanuit de Auteurswet bezit de maker van creatief werk automatisch het auteursrecht, tenzij hierover expliciet andere afspraken zijn gemaakt. Broncode valt onder creatief werk, dus het is belangrijk om goed vast te leggen wie (auteursrechtelijk) rechthebbende is van de geleverde broncode. Alleen de rechthebbende kan namelijk beslissen hoe (zijn deel van) de broncode gepubliceerd mag worden. Bedenk dat naast het auteursrecht met name ook het merkenrecht en databankenrecht in het spel kunnen zijn. In dit stuk wordt geconcentreerd op het auteursrecht, aangezien veel open source licenties het merkenrecht ook standaard al meenemen in hun voorwaarden.

Veel grote softwareprojecten bestaan uit verschillende componenten. Elk component kan meerdere ontwikkelaars hebben, die elk een deel van de (auteurs)rechten bezitten. Het is daarom essentieel om inzicht te hebben in de (auteurs)rechten op de broncode of in ieder geval zekerheid te hebben dat alle onderdelen onder een open source licentie zijn vrijgegeven. Zo worden (auteursrecht)schendingen zoveel mogelijk voorkomen.

Hou in ieder geval rekening met de volgende aandachtspunten als je aan de slag gaat met opensourcewerken:

- **Externe medewerkers** Wanneer externen werken aan broncode, maak dan expliciet dat de volledige rechten (auteursrechten en eventuele merkenrechten, databankrechten

en octrooirechten) bij de opdrachtgever komen te liggen. Bepalingen uit de standaard (inkoop)voorwaarden bieden daar onvoldoende juridische basis voor (bron).

- **Overdracht van broncode** Zorg dat je beschikt over de volledige rechten (auteursrechten en eventuele merkenrechten, databankrechten en octrooirechten) als je de broncode wil overdragen of wanneer je broncode overgedragen krijgt. Uitzondering is die broncode waar een open source licentie aan de broncode verbonden is. De overdracht van genoemde rechten moet altijd schriftelijk gebeuren daar waar van toepassing met een getekende overeenkomst en/of inschrijving in een relevant register. Als de rechten eerder niet zijn overgedragen, maar dat wel gewenst was, probeer deze alsnog te verkrijgen of een open source licentie aan de broncode te verbinden.

Marktverstoring

Bij het via open source beschikbaar stellen van software moet o.a. gekeken worden naar de Wet Markt en Overheid (Wet M&O). De overheid kan door het beschikbaar stellen van software concurreren met reeds in de markt aanwezige software. Als dit het geval is, moet de overheid zich houden aan de vier gedragsregels om concurrentievervalsing te voorkomen. Een van die gedragsregels schrijft voor dat de overheid alleen de broncode openbaar mag maken via open source als de integrale kosten worden doorberekend aan de eindgebruiker. Met de integrale kosten wordt bedoeld alle kosten die samenhangen met het aanbieden van de software aan de eindgebruiker. Denk daarbij aan bijvoorbeeld publicatie – en ontwikkelingskosten.

Of de overheid zich moet houden aan de (vier gedragsregels uit de) Wet M&O zal per geval onderbouwd moeten worden. Daarbij zal de Wet M&O sneller van toepassing zijn als de overheid de broncode als product op de markt exploiteert dan wanneer de overheid de broncode enkel openbaar maakt ter inzage. Mocht er sprake zijn van een wettelijke verplichting voor de overheid tot openbaarmaking van de broncode op grond van de Wet open overheid (Woo) of de Wet hergebruik van overheidsinformatie (Who) zal goed gekeken moeten worden naar de onderlinge verhouding tussen deze wetten enerzijds en de Wet M&O anderzijds.

In sommige gevallen kan software die door een overheidsorgaan in het kader van haar overheidstaak wordt gebruikt buiten de werking van de Wet M&O vallen. Artikel 25h, tweede lid, van de Mededingingswet, biedt namelijk een mogelijke uitzondering voor levering van goederen of diensten door bestuursorganen als deze zijn bestemd voor de uitvoering van een publiekrechtelijke taak. Of bepaalde software daadwerkelijk onder deze uitzonderingsgrond valt, en derhalve open source beschikbaar kan worden gesteld, dient ook weer per geval

onderbouwd te worden en bij twijfel altijd te worden beoordeeld door een jurist.

Tot slot is het van belang om te benoemen dat er op dit moment een wetsvoorstel ligt om hoofdstuk 4b van de Mededingingswet (waarin de Wet M&O is opgenomen) aan te passen zodoende dat het aanbieden van open source software wordt uitgezonderd van de gedragsregel integrale kostendoorberekening. Achtergrond van deze wijziging is dat overheden gemakkelijker de broncode van open software kunnen publiceren waarmee maatschappelijke voordelen gerealiseerd kunnen worden. Omdat open source software per definitie gratis is kan de gedragsregel 'integrale kostprijs doorberekening' een belemmering vormen voor een bestuursorgaan om daadwerkelijk tot publicatie over te gaan (bron: Memorie van toelichting, Wijziging van de Mededingingswet in verband met aanpassing van de bepalingen over de markt en overheid, 35985-1). Op dit moment is het onduidelijk of en wanneer deze wetswijziging wordt doorgevoerd.

Archiefwet

Duurzame toegankelijkheid van overheidsinformatie is het uitgangspunt van de Archiefwet 2026. Overheidsinformatie moet vindbaar, beschikbaar, leesbaar, interpreteerbaar, betrouwbaar en toekomstbestendig zijn. Voor iedereen die daar recht op heeft en voor zo lang als noodzakelijk is. De Archiefwet gaat ervan uit dat overheidsinformatie openbaar moet zijn en dat burgers, onderzoekers, media, journalisten en ambtenaren moeten kunnen zien wat de overheid doet en heeft gedaan. Het moet voor de toekomst mogelijk zijn om onderzoek te kunnen doen naar de achtergrond van overheidsbesluiten en deze te kunnen reconstrueren. Ook is het nodig om lessen te kunnen trekken uit ervaringen uit het verleden.

Informatie kan vóór overbrenging naar een archiefbewaarplaats al gerubriceerd zijn, bijvoorbeeld als "Confidentieel" of "Geheim". Deze rubricering heeft als doel om voortijdige openbaarmaking te voorkomen. Na overbrenging naar de archiefbewaarplaats vervalt de formele rubricering, maar dat betekent niet automatisch dat de informatie direct voor iedereen toegankelijk is. De zorgdrager kan alsnog besluiten om de documenten beperkt openbaar te maken. Zo blijven notulen uit de ministerraad 20 jaar geheim. Na die periode moeten ze (beperkt) openbaar gemaakt worden op een manier die duurzame toegankelijkheid ondersteunt. Dit betekent bijvoorbeeld dat ze onafhankelijk zijn van technologische ontwikkelingen. Aangezien technologische ontwikkelingen razendsnel gaan is het belangrijk om duurzame toegankelijkheid een integraal onderdeel van het proces te maken.

Stel dat een overheidsinstantie een software oplossing ontwikkelt (propriëtair) voor een kritisch

proces zoals belastingaangiften of identiteitsverificatie. Volgens de Archiefwet moeten blijvend te bewaren documenten en informatie na een bepaalde termijn worden overgebracht naar een archiefbewaarplaats. Dit kan ook gelden voor digitale informatie waaronder ook broncode. Als de broncode van zo'n systeem openbaar wordt gemaakt rijst de vraag: Hoe zorgen we ervoor dat deze code nog beschikbaar, leesbaar, interpreteerbaar, betrouwbaar en toekomstbestendig is?

De Archiefwet maakt geen expliciet onderscheid tussen open source en propriëtaire broncode, maar open source maakt het wel makkelijker om te voldoen aan de eisen voor duurzame toegankelijkheid. Open source geeft een bredere waarborg dat informatie open en controleerbaar, duurzaam en vooral niet afhankelijk is van een gesloten systeem of één partij. Met open source i.c.m. open standaarden is de kennis achter bepaalde techniek inzichtelijk. Als deze aangevuld worden met documentatie en metadata kunnen toekomstige gebruikers de context en functionaliteit beter begrijpen. Mocht in de toekomst PDF niet meer bestaan, dan zouden we met open standaarden beschrijvingen en open source makkelijker een nieuwe implementatie kunnen maken om PDF opnieuw uit te kunnen lezen.

Europees

De Verordening Cyberweerbaarheid / Cyber Resilience Act (CRA)

Het is van belang te vermelden dat met de inwerkingtreding van de Verordening Cyberweerbaarheid (Verordening 2024/2847/EU) een productaansprakelijkheid voor beveiligingslekken in software is ontstaan.

Kort samengevat betekent dit dat bij het op de Europese markt brengen van "producten met digitale elementen" - kortweg alles waar software in zit, ook de software zelf - een productaansprakelijkheid geldt. Deze aansprakelijkheid bestaat onder andere uit de verplichtingen om:

- Ontwerp, ontwikkeling en bouw conform de vereisten voor informatiebeveiliging van Annex I van de CRA;
- Risico-beoordeling gedurende de gehele levenscyclus van het product ten aanzien van informatiebeveiligingsrisico's;
- Actualisatie van bovengenoemde risico-beoordeling;
- Opname van de risico-beoordeling in de productdocumentatie;

- Het betrachten van gepaste zorg bij de integratie van componenten van derden;
- Het doorgeven van ontdekte beveiligingskwetsbaarheden in componenten van derden aan die derden (dat kunnen ook zogenaamde “open-source stewards” zijn);
- Het systematisch documenteren van beveiligingsaspecten van de software;
- Het effectief afhandelen van beveiligingskwetsbaarheden die gemeld worden;
- Gedurende ten minste vijf jaar het product ondersteunen in de vorm van beveiligingsupdates;
- Het gedurende ten minste tien jaar beschikbaar houden van gepubliceerde beveiligingsupdates;
- Het uitvoeren van conformiteitesbeoordelingen daar waar sprake is van CE-conformiteitschema’s;
- Het melden van beveiligingskwetsbaarheden die daadwerkelijk uitgebuit worden aan nationale autoriteiten (CSIRTS) en de Europese toezichthouder ENISA.

Het voert tever om de hele CRA weer te geven. Voor nu is van belang dat deze productaansprakelijkheid door de Europese wetgever met opzet genuanceerd is voor open source ontwikkelingen, om zo individuele ontwikkelaars hier niet mee te belasten. Daarmee is een nieuw begrip in het Europese productaansprakelijkheidsrecht geïntroduceerd: de “open-source steward”. Zij hebben de bijzondere rol om open source ontwikkelaars te beschermen, zowel individuele als MKB-ontwikkelaars. Voor andere partijen in de waarde-keten is het model gelijk aan de reguliere productaansprakelijkheidswetgeving, dus “producenten”, “importeurs”, “distributeurs” blijven onverkort onderhevig aan de eisen van de CRA.

Bijdragers

Met dank aan alle bijdragers:

- Maurice Hendriks (Hoofdauteur; Ministerie van Volksgezondheid, Welzijn en Sport)
- Walter van Holst (Hooghiemstra & Partners)

Aanvullend hebben juristen van MinVWS en het Nationaal Archief meegewerkt aan dit document.

Deze tekst is beschikbaar onder de CC-BY-4.0
Collaborate on HackMD