Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2022–2023

36 239 Voorstel voor een Verordening betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordening (EU) 2019/1020

B

BRIEF VAN DE VOORZITTER VAN DE VASTE COMMISSIE VOOR JUSTITIE EN VEILIGHEID

Aan vicevoorzitter Šefčovič van de Europese Commissie

Den Haag, 13 december 2022

De leden van de vaste commissie voor Justitie en Veiligheid hebben in hun commissievergadering van 15 november 2022 beraadslaagd over het door de Europese Commissie voorgestelde Voorstel voor een verordening betreffende horizontale cyberbeveiligingsvereisten[1]. De leden van de fracties van **GroenLinks**, **Partij van de Arbeid** (PvdA), de **Socialistische Partij** (SP) en de **Partij voor de Dieren** (PvdD) gezamenlijk hebben naar aanleiding van het voorstel enkele vragen. Ook het lid van de **Onafhankelijke Senaatsfractie** (OSF) heeft vragen naar aanleiding van het voorstel.

Vragen van de leden van de fracties van GroenLinks, PvdA en SP en PvdD gezamenlijk

De leden van de fracties van GroenLinks, PvdA en de SP gezamenlijk hebben met interesse kennisgenomen van het voorstel. Zij ondersteunen het uitgangspunt dat er duidelijke algemene kaders moeten komen voor de veiligheid van digitale producten en diensten. De leden hebben wel een aantal vragen over onder andere de impact van de verordening op vrije en opensourcesoftware en over de effectieve handhaving van het voorstel.

Vrije en open source software

De leden zijn blij om in considerans nummer 10 van het voorstel te lezen dat vrije en opensourcesoftware, die buiten het kader van handelsactiviteiten wordt ontwikkeld of geleverd, moet zijn uitgezonderd van toepassing van de verordening.[2] De leden constateren dat het ontwikkelen van vrije en open source software op een hele diverse manier gebeurt. Zij

[1] COM(2022)454.
[2] COM(2022)454, p. 16.

kst-36239-B
ISSN 0921 - 7371
's-Gravenhage 2022

zijn daarom bang dat niet duidelijk genoeg afgebakend is wanneer er sprake is van vrije software, ontwikkeld of geleverd in het kader van een handelsactiviteit. Onderschrijft de Europese Commissie dat duidelijkheid voor opensource-ontwikkelaars omtrent toepasbaarheid van de verordening, essentieel is om te zorgen dat dit voorstel geen onvoorziene gevolgen heeft voor opensourcesoftware in Europa? Vanuit welke afwegingen is de Europese Commissie gekomen tot de tekst van het onderhavige voorstel?

De leden zijn blij dat in de considerans nog een aantal voorbeelden is gegeven wanneer er sprake kan zijn van handelsactiviteit voor software. De leden horen graag of volgens de Europese Commissie de volgende voorbeelden in overwegende mate ook onder «handelsactiviteit» zouden kunnen vallen:

1. Het ontvangen van vrijwillige, onvoorwaardelijke donaties door gebruikers van de software.
2. Het ontvangen van prestatieafhankelijke donaties («feature bounties»).
3. Ontwikkelaars die gesponsord worden, bijvoorbeeld door materialen te krijgen of reiskosten voor conferenties vergoed te krijgen.
4. Het gratis uitlenen van apparatuur ter bevordering van de ontwikkeling van de opensourcesoftware.

Daarnaast zullen er natuurlijk (grote) vrije en opensourcesoftwareprojecten zijn die wel onder de werking van de Cyber Resilience Act (CRA) zullen vallen. De leden vinden dat uiteraard niet bezwaarlijk; grote opensourceprojecten waar geld aan verdiend wordt, moeten immers ook veilig zijn. Wel zien zij in de uitvoering hiervan enkele onduidelijkheden. Wie is verantwoordelijk voor de naleving van de verplichtingen uit hoofdstuk 2 van het voorstel als een – door een collectief gemaakt – softwareproduct door een marktpartij «op de markt» wordt gebracht[3], bijvoorbeeld door het verlenen van betaalde ondersteuningsdiensten?[4] Is dat dan de marktpartij die de ondersteuningsdiensten levert, het collectief van vrijwilligers die de software schrijft, of beide? Is het onder het huidige voorstel mogelijk dat een enkele vrijwilliger aansprakelijk gesteld wordt, omdat een andere partij software waaraan hij heeft bijgedragen in de handel brengt?

De leden vinden het belangrijk dat de zorgen van de vrije en opensourcesoftwaregemeenschap weggenomen kunnen worden en dat Unieburgers goed ingelicht wordt in welke gevallen een product of softwareproject onder de voorwaarden van dit voorstel zullen vallen. Dit om «chilling effects» te voorkomen en de administratieve last te verlagen. Welke acties zal de Europese Commissie ondernemen om te zorgen dat de effecten van de verordening duidelijk zullen zijn en de administratieve lasten voor compliance overzichtelijk blijven voor de vrije en opensourcesoftwaregemeenschap? Zou de Europese Commissie een concrete handreiking kunnen doen aan de vrije en opensourcesoftwaregemeenschap door richtlijnen op te stellen wanneer, en in hoeverre, opensourcesoftwareprojecten binnen de reikwijdte van de verordening zullen vallen?

Onderstreept de Europese Commissie het belang van een gezonde en actieve opensourcesoftwaregemeenschap in Europa, zowel vanuit het perspectief om minder afhankelijk te zijn van software buiten Europa, als vanuit het perspectief van digitale innovatie? Zo ja, heeft de Europese

[3] Artikel 3 (21), p. 37.
[4] Overweging 10, p. 16.

Commissie acties ondernomen, of is zij van plan acties te ondernemen, om het speelveld voor opensourcesoftware en -hardware te verbeteren in de EU?

De leden merken ook op dat veel vrije en opensourcesoftware die gratis beschikbaar wordt gemaakt buiten handelsactiviteit vervolgens weer gebruikt wordt in commerciële producten door andere partijen. Veel software waar veel mensen (indirect) van afhankelijk zijn, worden (grotendeels) ontwikkeld door vrijwilligers. Heeft de Europese Commissie overwogen om in de CRA bepalingen op te nemen die fabrikanten die opensourcesoftware gebruiken aan te moedigen om vrijwillige upstream-opensourcesoftware-ontwikkelaars te ondersteunen in het realiseren van de verplichtingen uit de CRA? Zo ja, waarom is dit niet gerealiseerd? Zo nee, zou de Europese Commissie positief er tegenover staan om zulke prikkels toe te voegen aan de CRA?

Handhaving

De leden vroegen zich af hoe zij de verhouding tussen de CRA en de voorgestelde vernieuwde productaansprakelijkheidsrichtlijn moeten zien. Op welke manier biedt de CRA dan wel de nieuwe productaansprakelijkheidsrichtlijn voldoende mogelijkheden voor eindgebruikers om nakoming van de verplichtingen uit de CRA af te dwingen?

Levensduur[5]

De leden zijn blij om te lezen dat de verordening een verplichting inhoudt om voor een bepaalde duur kwetsbaarheden op te lossen. De gekozen duur van ten hoogste vijf jaar, of de verwachte levensduur als dat korter is, vinden de leden echter onbegrijpelijk in het licht van de duurzaamheidsambities van de EU. Veel fysieke producten zijn immers volledig afhankelijk van veilige software. Een korte ondersteuningstermijn van de software op dergelijke producten kan onnodige verspilling in de hand werken. Waarom is er gekozen voor een zo algemene termijn, in plaats van een termijn die productafhankelijk is? En waarom is er specifiek gekozen voor een maximumtermijn van 5 jaar?

Daarnaast zullen gebruikers na het einde van deze wettelijke ondersteuningstermijn mogelijk gebruik willen blijven maken van het product met digitale elementen. Welke mogelijkheden biedt de CRA aan gebruikers om te zorgen dat ze ook na deze termijn veiligheidsupdates kunnen krijgen, eventueel van een andere partij dan de oorspronkelijke fabrikant? Hoe kijkt de Europese Commissie ernaar om een verplichting te stellen om broncode, inclusief voorbereidend materiaal zoals «toolchains» en compilatiegegevens, na een bepaalde termijn beschikbaar te moeten stellen als een fabrikant geen veiligheidsupdates meer wil leveren?

Vragen van het lid van de fractie van de OSF

Het lid van de OSF heeft kennisgenomen van het voorstel om sectorbreed de digitale beveiliging te verhogen en daarmee de algehele ICT-infrastructuur minder kwetsbaar te maken. Hij ziet deze verordening als het toevoegen van het recht op cyberbeveiliging en stellen van een updateverplichting. Er zijn wel meerdere onduidelijkheden welke het lid graag meer verhelderd zou willen zien.

[5] Artikel 23 (2), p. 51–52

Spoorboekje

Aanvullend, welke route wordt geboden voor nationale initiatieven om ook op Europese schaal uitvoerbaar te worden? Hierbij kunnen we bijvoorbeeld denken aan (aanvullende) richtlijnen, implementaties en ook (subsidie)regelingen.

Voorziet de Europese Commissie de wens en de mogelijkheid om een bredere procedure te doorlopen? Hierbij kan gedacht worden aan bijvoorbeeld meervoudige consultatie of installatie van een adviesorgaan vanuit de sector. Een bredere procedure, mogelijk zelfs cyclisch, zou kunnen bijdragen aan de (door)ontwikkeling van de criteria en de sectorbrede voorlichting van de standaard die wordt nagestreefd. Ook om, in de reikwijdte van de CRA, in afstemming te blijven/brengen met andere Unie wetgevingsinstrumenten. Zo ja, hoe ziet de Europese Commissie dat dan voor zich?

Cyberbeveiliging betreft zeer specialistische kennis, terwijl volksvertegenwoordiging in veel gevallen een lekenbestuur is. Zeker op dit vakgebied. Op welke wijze wordt gewaarborgd dat de CRA als beleid ook uitvoerbaar zal zijn? Hoe wordt voorkomen dat deze verordening flopt? Er is veel geschaad vertrouwen als het gaat om overheden en haar ICT-projecten. Hoe wil de Europese Commissie haar geloofwaardigheid herwinnen/bewijzen, zodat ze ook sectorbreed steun krijgt om met deze verordening de cyberbeveiliging daadwerkelijk naar een hoger niveau te tillen?

Handhaving

In het voorstel blijft onduidelijk hoe en met welke reikwijdte en daadkracht de CRA zal worden gehandhaafd. In het arsenaal van middelen die nodig zouden kunnen zijn, zou ook kunnen geworden gedacht aan handelingen die (momenteel) voorbehouden zijn tot het nationale recht. Kan de Europese Commissie inzicht geven op de rechtsgevolgen die er kunnen voortkomen in de naleving van de CRA dan wel schenden van de CRA?

Startups en innovatie

De verordening verzoekt aanbieders om over te gaan tot certificering en het verkrijgen van een label. Zo ook voor startups en innovatie binnen de sectoren die onder deze verordening zullen vallen. Een zelfassessment van geschat 18.400 euro en/of een conformiteitsbeoordeling door een derde partij van geschat 25.000 euro kunnen worden gezien als aanzienlijke investeringen. Is de Europese Commissie voornemens om hierin een subsidieregeling te voorzien? Of zijn er uitzonderingsregels of verminderde reikwijdte te verwachten om de administratieve lasten te verlichten?

Daar waar Europese ontwikkelaars geconfronteerd worden met de CRA, is er een aannemelijke kans dat wereldwijd denkende spelers binnen de sector, innovatie buiten Europa gaan plaatsen. Is er bij de Europese Commissie inzicht in hoe de CRA invloed zal gaan hebben op arbeidsmarkt van de sector en onze globale positie binnen de kenniseconomie? En/of heeft de Europese Commissie vertrouwen in de realisatie van een wereldwijde standaard met deze verordening, waarmee ook niet-Europese aanbieders kunnen worden geconformeerd? Voorziet ze dat aanbieders de Europese markt (voorlopig) zullen gaan mijden, met gevolg van verminderd aanbod, keuzevrijheid en maatwerk?

Eerlijke concurrentie

De nalevingskosten worden als 2% van de omzet geschat. Berekening: 29 miljard ten opzichte van 1.485 miljard. Omdat een zelfassessment of conformiteitsbeoordeling geschat wordt op 18,4 tot 25 duizend euro, kan daarmee worden afgeleid dat voor dit specifieke certificaat er een omzet van boven de 1 miljoen euro als marktcomfort wordt ingeschaald. Heeft de Europese Commissie toezichthouders op de markten om een zienswijze gevraagd?

Financiële consequenties

Qua financiële consequenties voor de nationale overheid en/of medeoverheden, evenals de gevolgen van regeldruk voor bedrijfsleven en de burger worden miljardenbedragen voorzien. Zowel voor kosten als voor kostenbesparing. Zodra de gevolgen van de invoering van deze verordening duidelijk worden, is de Europese Commissie voornemens om hiervoor een compensatieregeling in te richten? Zo ja, welke doelgroepen (zoals gemeenten of midden- en kleinbedrijf) en om welke redenen, zullen dan worden gecompenseerd? Op welke wijze zal dit in de begroting worden ingepast en/of hoe zal dit herleidbaar zijn?

Gijzeling van gegevens en systemen

In de laatste jaren worden ook overheden en publieke instellingen geconfronteerd met cyberbeveiligingsincidenten. Kan de Europese Commissie aangeven hoe deze situaties (door de verordening) voorkomen hadden kunnen worden? Welke criteria worden gehanteerd, ook bij werkwijzen wanneer gegevens gegijzeld worden en systemen overgenomen?

Actieve uitbating zwakheden door derden

Met de oorlog in Oekraïne is Europa wakker geschud dat er ook een digitaal front is. Hoe wil Europa deze verordening inzetten om zich te wapenen in de «digitale oorlog»? Welke beperkingen en/of vrijheden van de nationale veiligheids- en inlichtingendiensten komen met de CRA in een ander daglicht te staan?

Bescherming van klokkenluiders en ethische hackers

Zwakten in systemen worden altijd door mensen ontdekt. Leveranciers hebben economische belangen bij het (ogenschijnlijk) ontbreken van zwakheden. Op welke wijze worden klokkenluiders en ethische hackers mede door deze verordening in bescherming genomen?

De leden van de vaste commissie voor Justitie en Veiligheid zien uw reactie met belangstelling tegemoet.

De Voorzitter van de vaste commissie voor Justitie en Veiligheid,
M.M. de Boer