Briefingpaper soevereiniteitsbepalingen EUCS

Online Trust Coalitie, juni 2023

Doelstelling van deze briefingpaper is om bestuurders van organisaties die clouddiensten gebruiken in staat te stellen om inzicht te krijgen in de vraag wat de mogelijke consequenties voor de organisatie zijn van de soevereiniteitsbepalingen die zijn opgenomen in het Europese concept certificeringsschema voor de cybersecurity van clouddiensten *(EUCS).*

In 2019 is de EU Cybersecurity Act *(Verordening EU 2019/881 dd 17 april 2019)* van kracht geworden. Deze verordening regelt de instelling van ENISA als het Agentschap van de Europese Unie voor Cyberbeveiliging *(Titel 2)* en geeft een cyberbeveiligingscertificeringskader *(Titel 3).* In het kader van dit cyberbeveiligingscertificeringskader wordt ENISA door de Europese Commissie opgedragen om certificeringsschema's te maken voor de cyberveiligheid van ICT-producten, -diensten en -processen. Deze schema's bevatten cybersecuritynormen voor drie niveaus van certificering *(assurance levels):* Basic, Substantial en High.

Het maken van deze schema's gebeurt door ENISA met ondersteuning van Ad-hoc werkgroepen waarin specialisten, belanghebbenden en overheidsvertegenwoordigers deelnemen. Een van de eerste certificeringsschema's die door ENISA wordt gemaakt is voor de cybersecurity van clouddiensten.

De ontwikkeling van het certificeringsschema voor clouddiensten *(het EUCS)* is begin 2020 gestart en een eerste concept is in december 2020 voor publieke consultatie aangeboden. Na de publieke consultatie zijn de in het schema opgenomen beveiligingseisen ingrijpend herzien en zijn deze eisen en de methodologie voor de conformiteitsbeoordeling door ENISA ter review aan CEN/CENELEC voorgelegd. Los hiervan heeft ENISA in opdracht van de Europese Commissie een bijlage J aan het schema toegevoegd. Deze bijlage bevat een aantal aanvullende bepalingen die clouddiensten die tegen assurance level "High" gecertificeerd worden, moeten beschermen tegen de invloed van niet-Europese regelgeving. Dit zijn de zogenoemde INL-criteria: Immunity for Non-EU Law.

Door verschillende belanghebbenden wordt gewaarschuwd voor de ingrijpende gevolgen van de INL-criteria. Belangrijkste reden is dat zij de facto de EU-markt voor tegen assurance level "High" gecertificeerde diensten ontoegankelijk maken voor niet-Europese aanbieders die op dit moment de grootste partijen op deze markt zijn en hoogwaardige clouddiensten leveren. Maar ook voor Europese aanbieders en afnemers van clouddiensten die gebruik maken van diensten van niet-Europese partijen zullen de gevolgen ingrijpend zijn. Te denken valt daarbij aan significant hogere kosten of het niet meer beschikbaar zijn van diensten. De stellige verwachting is daarbij dat veel leveranciers van clouddiensten zich genoodzaakt zullen zien om hun diensten te laten certificeren tegen assurance level "High" omdat zij verwachten daartoe op termijn gedwongen te zullen worden of omdat zij bij tendens niet op achterstand willen staan.

Nederland is van mening dat alvorens deze INL-criteria definitief in het schema worden opgenomen, er een economische impactanalyse moet worden uitgevoerd. Op basis van deze

impactanalyse moet er een politieke discussie in Europa plaatsvinden over de wenselijkheid van deze INL criteria. Nederland heeft het initiatief genomen om deze problematiek middels een zogenoemde non-paper aan de lidstaten voor te leggen. Inmiddels is dit non-paper door een groot aantal lidstaten ondertekend. Zie de bijlage voor het Nederlandse non-paper.

Medio mei 2023 heeft de Europese Commissie een nieuwe versie van het EUCS vrijgegeven waarin de INL bepalingen zijn hernoemd in PUA *(Protection of European Data against Unlawful Access)* bepalingen terwijl er tevens vier zogenoemde Evaluation Levels *(CS-EL1 t/m 4)* zijn geïntroduceerd waarmee de facto een extra assurance level *(High+)* wordt geïntroduceerd. De PUA bepalingen gelden met name voor CS-EL 3 en CS-EL4 die gekoppeld zijn aan assurance level “High” en in beperkte mate ook voor de andere evaluation levels.

Het kernteam van de Online Trust Coalitie is van mening dat er een significante impact te verwachten is voor zowel de aanbieders van clouddiensten, als de afnemers ervan. Puntsgewijs is dit als volgt samen te vatten:

- De markt *(zowel aanbieders als gebruikers van cloud diensten)* is op dit moment nog niet voorbereid op de impact van soevereiniteitsbepalingen doordat er voor belangrijke *(dominante)* niet-europese diensten op dit moment geen Europese alternatieven voorhanden zijn.
- PUA bepalingen gelden met name voor assurance level “High” certificeringen met een verbijzondering in evaluation levels 3 en 4. De markt verwacht dat certificering tegen assurance level “High” en CS-EL4 voor clouddiensten de standaard zal worden.
- Dit vraagt een enorme omschakeling van de markt, die, zonder zorgvuldig beleid, tot uitval van aanbieders uit de markt en op korte termijn tot uitval van aanbod leidt.
- Het opwerpen van blokkades voor met name dominante VS aanbieders zal, zonder zorgvuldig beleid, kunnen leiden tot prijsstijgingen van hun diensten als gevolg van technisch herontwerp, juridische constructies, en organisatorische inrichtingen *(er worden percentages van meer dan 25% genoemd)*. Een impactanalyse is dus belangrijk om de te verwachten gevolgen in kaart te brengen.
- Macro-economisch loopt de EU het risico dat de EU, zonder analyse en aanvullend beleid, achter gaat lopen op het gebied van innovatie omdat daarvoor benodigde technologie niet of later voor EU partijen beschikbaar komt.
- De vrees bestaat dat als PUA/INL bepalingen op korte termijn worden ingevoerd, dit gaat leiden tot hoge migratiekosten voor afnemers van clouddiensten door huidig gebrek aan transparantie, interoperabiliteit en portabiliteit.
- Indien komende EU regelgeving ook een verplichtend karakter gaat geven aan certificering, dan kan dit grote impact hebben op de beschikbaarheid van kritieke services van grote partijen en daarmee direct impact hebben op het functioneren en de concurrentiepositie van gebruikers van clouddiensten.
- Samenvattend is de conclusie dat het op dit moment opnemen van PUA bepalingen in het EUCS grote impact zal hebben voor zowel individuele partijen als de EU markt als geheel. Voor het verantwoord opnemen van de bepalingen is een analyse van de impact, van de ontwikkelingen op de markt en scenario’s *(beleid)* nodig. De exacte grootte van die impact en de details is/zijn op dit moment onvoldoende duidelijk.
- Onze aanbeveling is dan ook om door de Europese Commissie een economische impact assessment op te laten stellen op EU niveau waarin de verschillende scenario’s worden uitgewerkt en de gevolgen voor de lidstaten geanalyseerd worden. In afwachting daarvan zouden de PUA/INL bepalingen buiten het EUCS moeten blijven zodat invoering van het EUCS door kan gaan en de PUA/INL bepalingen later na politieke besluitvorming in een overeengekomen vorm gerealiseerd kunnen worden.

Het kernteam van de Online Trust Coalitie voorziet de bovenstaande risico's voor de cloudmarkt in Nederland/Europa als geheel. Voor de lopende discussie binnen de European Cybersecurity Certification Group *(ECCG = het adviescollege voor de Europese Commissie inzake cybersecurity certificering met vertegenwoordigers van de lidstaten)* zou het helpen als organisaties en bedrijven zo snel mogelijk individueel bepalen wat de gevolgen voor hun organisatie en bedrijfstak kunnen zijn. Daarmee kan de verwachte impact al voor een deel worden onderbouwd. Deze informatie kan dan via de Nederlandse vertegenwoordiger in de ECCG *(de RDI: Rijksinspectie voor de Digitale Infrastructuur)* worden ingebracht om de Europese Commissie te bewegen tot het uitvoeren van een economische impactanalyse. De besluitvorming in Europa over het EUCS *(en dus over de PUA criteria)* zal naar verwachting de komende maanden plaatsvinden. Het is dus belangrijk dat aanbieders en afnemers van clouddiensten hun bezwaren zo snel mogelijk kenbaar maken.

Op dit moment bestaat er in Europa nog geen verplichting om clouddiensten te certificeren of om uitsluitend gecertificeerde clouddiensten te gebruiken. De kans is echter aanwezig dat in het kader van andere Europese regelgeving of bijvoorbeeld aanbestedingsregels, in de toekomst deze plicht wel zal ontstaan of onvermijdelijk wordt voor zowel aanbieders als afnemers. Hoewel dit door de Europese Commissie op dit moment ontkend wordt, gaan wij er in onze scenario's vanuit dat dit wel gaat gebeuren. Bijvoorbeeld in de uitwerking van de Europese NIS2 richtlijn, de Europese Digital Operational Resilience Act *(DORA)*, de Cyber Resilience Act of de Europese Health Data Space Regulation. De Cybersecurity Act geeft de Europese Commissie hiertoe in artikelen 56.2 en 56.3 de mogelijkheid.

Voor vragen kunt u contact opnemen met het kernteam van de Online Trust Coalitie:
info@onlinetrustcoalitie.nl