Fiche 1: Verordening Informatiebeveiliging in de instellingen, organen en instanties van de Unie

1. Algemene gegevens

a) Titel voorstel

Voorstel voor een verordening van het Europees Parlement en de Raad betreffende informatiebeveiliging in de instellingen, organen en instanties van de Unie

b) Datum ontvangst Commissiedocument

22 maart 2022

c) Nr. Commissiedocument

COM(2022) 119

d) EUR-lex

EUR-Lex - 52022PC0119 - NL - EUR-Lex (europa.eu)

e) Nr. impact assessment Commissie en Opinie Raad voor Regelgevingstoetsing

SWD(2022) 65 final, SWD(2022) 66 final

f) Behandelingstraject Raad

Raad Algemene Zaken

g) Eerstverantwoordelijk ministerie

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

h) Rechtsbasis

Artikel 298 van het Verdrag betreffende de werking van de Europese Unie (VWEU)
Artikel 106a van het Verdrag tot oprichting van de Europese Gemeenschap voor Atoomenergie (Euratom-Verdrag)

i) Besluitvormingsprocedure Raad

Gekwalificeerde meerderheid

j) Rol Europees Parlement

Medebeslissing

2. Essentie voorstel

a) Inhoud voorstel

Het voorstel voor een verordening van het Europees Parlement en de Raad betreffende informatiebeveiliging in de instellingen, organen en agentschappen van de Unie (hierna: EU IOA's) heeft als doel het tot stand brengen van een hoog gemeenschappelijk niveau van beveiliging voor

gerubriceerde informatie van de Europese Unie (EUCI) en niet-gerubriceerde informatie die door de EU IOA's worden verwerkt en opgeslagen. De Commissie geeft meerdere redenen die aanleiding geven tot deze verordening. Ten eerste hebben de EU IOA's op dit moment ofwel elk hun eigen voorschriften op het gebied van informatiebeveiliging, ofwel helemaal geen voorschriften op dat gebied. Hierdoor is het complex informatie onderling uit te wisselen en bestaan er discrepanties tussen verschillende soorten voorschiften. Ten tweede is de huidige regelgeving voor informatiebeveiliging in veel gevallen verouderd en niet toegespitst op de huidige manier van werken en de ontwikkeling van nieuwe technologieën. Dit maakt de informatie kwetsbaar voor aanvallen van met name statelijke actoren met een offensief cyberprogramma tegen EU-belangen. Ten derde neemt de hoeveelheid gevoelige niet-gerubriceerde informatie en EUCI in het bezit van de EU IOA's toe. Deze informatie is aantrekkelijk voor statelijke actoren en de dreiging gericht op deze informatie neemt toe. Het is daarom van belang dat deze informatie beter beveiligd wordt. Dit beoogt tevens bij te dragen aan een onafhankelijk en efficiënt bestuur van de Unie en betere preventie van (informatie)beveiligingsincidenten en datalekken.

Daarom poogt de voorgestelde verordening het niveau van informatiebeveiliging van de EU IOA's te verhogen door alle voorschriften op het gebied van informatiebeveiliging te harmoniseren in één verordening. De reeds bestaande informatiebeveiligingsregels voor EUCI worden in de voorgestelde verordening gemoderniseerd. Hierbij wordt rekening gehouden met nieuwe technologieën en de ontwikkeling van thuiswerken als structurele praktijk. De verordening schrijft onder andere voor dat voor de beveiliging van EUCI gebruik gemaakt moet worden van goedgekeurde cryptografische producten. De Raad is verantwoordelijk voor het bijhouden van een lijst met goedgekeurde producten, op basis van input van de nationale veiligheidsautoriteiten.

In aanvulling op deze modernisering van het bestaande rubriceringssysteem voor EUCI introduceert de verordening een nieuwe categorie informatie: 'niet-gerubriceerde informatie' ('*non-classified information*'). Dit is een nieuwe ontwikkeling. Tot op heden bestaan er namelijk geen informatiebeveiligingsregels voor de omgang met niet-gerubriceerde informatie. De categorie 'niet-gerubriceerde informatie' wordt onderverdeeld in 1) 'informatie voor openbaar gebruik' ('*information for public use*'); 2) 'normale informatie' ('*normal information*') en 3) 'gevoelige niet-gerubriceerde informatie' ('*sensitive non-classified information*'). Hierbij dient opgemerkt te worden dat de definitie van de categorie 'gevoelige niet-gerubriceerde informatie'[1] nauwelijks verschilt van de definitie van de reeds bestaande rubricering EU-RESTRICTED[2]. Naast de geharmoniseerde informatiebeveiligingsregels voor gerubriceerde en niet-gerubriceerde informatie blijft het mogelijk voor EU IOA's om eigen merkingen te hanteren.

Verder wordt een structuur opgezet om efficiënte samenwerking tussen de EU IOA's op het gebied van informatiebeveiliging te bevorderen. Deze bestaat uit de oprichting van een interinstitutionele

[1] 'Gevoelige niet-gerubriceerde informatie' wordt gedefinieerd als: "informatie waarvan de ongeoorloofde openbaarmaking schade toe kan brengen aan legitieme particuliere en openbare belangen, met inbegrip van die van de instellingen en organen van de Unie, de lidstaten of van personen'

[2] EU-RESTRICTED wordt gedefinieerd als: "informatie en materiaal waarvan de ongeoorloofde openbaarmaking nadelig kan zijn voor de belangen van de Unie of van één of meer van haar lidstaten".

coördinatiegroep voor informatiebeveiliging (coördinatiegroep), waarin de beveiligingsautoriteiten van de EU IOA's vertegenwoordigd zijn. De coördinatiegroep draagt de verantwoordelijkheid voor het nader uitwerken van het informatiebeveiligingsbeleid. Ter verdere uitvoering van de voorgestelde verordening zal de coördinatiegroep vijf permanente thematische subgroepen oprichten. Deze subgroepen zullen verantwoordelijk zijn voor het beleid op specifieke expertisegebieden. Waar nodig kan de coördinatiegroep ook voor specifieke taken en voor een beperkte duur ad-hoc subgroepen creëren. De coördinatiegroep zal worden geadviseerd door een comité voor informatiebeveiliging ('Information Security Committee'). Dit comité zal bestaan uit de vertegenwoordigers van de nationale veiligheidsautoriteiten (*National Security Authority*, NSA) van elke lidstaat en zal worden voorgezeten door het secretariaat van de coördinatiegroep.[3]

In de voorgestelde verordening wordt het veiligheidsdirectoraat van de Commissie een meer centrale rol toebedeeld. Zo zal dit veiligheidsdirectoraat voorzien in het secretariaat van de coördinatiegroep en deze groep ook voorzitten. Daarnaast kunnen organen en instanties van de Unie een Service Level Agreement (SLA) afsluiten met de Commissie om informatiebeveiligingstaken uit te besteden of gezamenlijk in te kopen.

Parallel aan dit voorstel heeft de Commissie het voorstel gepubliceerd genaamd het Voorstel voor een verordening van het Europees Parlement en de Raad betreffende informatiebeveiliging in de instellingen, organen en instanties van de Unie. Het kabinet informeert de Tweede Kamer hierover in een apart BNC-fiche.

b) Impact assessment Commissie

In de impact assessment ter onderbouwing van het voorstel geeft de Commissie aan dat de verordening alleen van toepassing is op de EU IOA's en niet direct van toepassing is op de lidstaten. Daarom is de verwachting van de Commissie dat de verordening geen significante impact op de lidstaten zal hebben. Voor wat betreft de EU IOA's verwacht de Commissie dat de voorgestelde verordening leidt tot meer efficiëntie omdat beveiligingsmaatregelen beter op elkaar afgestemd zijn en de inkoop van beveiligingsmiddelen gecoördineerd zal plaatsvinden.

Wat betreft de financiële impact wordt verwacht dat een hoger niveau van informatiebeveiliging potentiële incidenten - met economische of reputatieschade als gevolg - voorkomt. De Commissie verwacht dat de kosten die gepaard gaan met de implementatie van de verordening gedekt kunnen worden vanuit bestaande programma's ter verbetering van informatiebeveiliging. Ter ondersteuning van de coördinatiegroep wordt een secretariaat opgezet en organisatorisch ondergebracht bij het veiligheidsdirectoraat van de Commissie. Hiertoe zullen 2 FTE worden aangesteld.

[3] In Nederland is de rol van *National Security Authority* (NSA) belegd bij het Nationaal Bureau voor Verbindingsbeveiliging (NBV) van de AIVD. De Beveiligingsautoriteit (BA) van Defensie treedt op als NSA voor het militaire domein inclusief het militair industrieel complex.

3. Nederlandse positie ten aanzien van het voorstel

a) Essentie Nederlands beleid op dit terrein

Voor de beveiliging van informatie geldt in Nederland een samenhangend pakket van regelingen. Voor de Rijksdienst[4] geldt het Besluit BVA-stelsel Rijksdienst[5] dat de integrale beveiliging en de verdeling van taken tussen BZK en andere ministeries regelt en inzoomt op de rol en bevoegdheden van de departementale Beveiligingsautoriteit (BVA) en de RijksBVA. Voor het Ministerie van Defensie is een uitzondering gemaakt op de toepasselijkheid van het besluit. Het departement is op het gebied van beveiliging eigenstandig, waardoor bevoegdheden, taken en functie van de BVA anders zijn ingericht[6]. Daarbij geldt dat al naar gelang de aard en inhoud van het onderwerp van beveiliging afstemming gezocht tussen de betrokken ambtenaren van Defensie en de (inter)departementale beveiligingsambtenaar. De BVA van Defensie maakt wel onderdeel uit van het BVA-beraad.

Voor de beveiliging van alle informatie bij de Rijksdienst, zowel gerubriceerd als ongerubriceerd, en informatieprocessen geldt het besluit Voorschrift Informatiebeveiliging Rijksdienst (VIR[7]). Dit definieert informatiebeveiliging en stelt eisen aan het departementale informatiebeveiligingsbeleid. Het belangrijkste element is de verplichting om de managementcyclus te doorlopen bij de uitvoering van het risicomanagement. Dit is verder uitgewerkt in de Baseline Informatiebeveiliging Overheid (BIO)[8]. De BIO beschrijft het basisniveau voor informatiebeveiliging van informatie en informatieprocessen[9] en geldt voor de gehele Nederlandse overheid (Rijksdienst, Gemeenten, Waterschappen en Provincies). De BIO is gebaseerd op de internationaal erkende en actuele ISO-normatiek[10]. De BIO stelt de keuze van maatregelen op grond van de indeling ISO27002[11] centraal. Om de beveiliging van ketenprocessen bij de overheid efficiënt te laten verlopen, stelt de BIO daarbinnen een aantal concrete maatregelen verplicht. Ook zijn maatregelen opgenomen waarvan uitvoering noodzakelijk is en verplichting een middel is om uitvoering van deze maatregelen te bewerkstelligen.

Specifiek voor gerubriceerde informatie bij de Rijksdienst geldt aanvullende regelgeving. Dit staat in het besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIR-BI)[12]. Het

---

[4] Tot de Rijksdienst wordt gerekend: de ministeries met de daaronder ressorterende diensten, bedrijven en instellingen

[5] *Stcrt.* 2020, 62845

6 Omdat Defensie een bijzondere positie binnen het BVA stelsel in neemt, liggen de toezichthoudende taken op defensie of de -industrie bij de BA defensie in diens hoedanigheid als NSA Defensie.

[7] *Stcrt.* 2007, 122

[8] *Stcrt*. 2020, 7857

[9] NB De BIO geldt dus ook voor gerubriceerde informatie.

[10] De internationale organisatie voor standaardisatie (ISO) is een internationale organisatie die normen vaststelt. De organisatie is een samenwerkingsverband van nationale standaardisatieorganisaties in 163 landen.

[11] De ISO27002-standaard is een best practice van beveiligingsmaatregelen ('controls') om informatiebeveiligingsrisico's aan te pakken met betrekking tot vertrouwelijkheid, integriteit en beschikbaarheid van de informatievoorziening.

[12] *Stcrt.* 2013, 15497

VIR-BI schrijft op hoofdlijnen de te treffen beveiligingsmaatregelen voor de verwerking en opslag van gerubriceerde informatie, aanvullend op de BIO. Het VIR-BI schrijft voor dat gerubriceerde informatie die krachtens een internationaal verdrag of overeenkomst is verkregen, de toegekende rubricering behoudt en wordt beveiligd volgens het overeenkomstige nationale beveiligingsniveau. Voor zover voor de beveiliging van dergelijke informatie als gevolg van het verdrag of de overeenkomst afwijkende of verdergaande beveiligingsbepalingen bestaan, worden deze bepalingen toegepast.

Er is een verdrag afgesloten tussen de EU en de lidstaten waarin de taken en verantwoordelijkheden in relatie tot de beveiliging van EUCI zijn vastgelegd.[13] Hieruit volgt dat in elke lidstaat een nationale veiligheidsautoriteit is aangesteld, belast met het houden van toezicht op de beveiliging van EUCI, het leveren van beleidsbijdragen ten behoeve van de beveiliging van EUCI en het afgeven van persoonlijke veiligheidsmachtigingen (*clearance)*.

b) Beoordeling + inzet ten aanzien van dit voorstel

Het kabinet staat overwegend positief tegenover het voorstel. Het kabinet herkent de geschetste problematiek en erkent de noodzaak voor het verhogen van het niveau van informatiebeveiliging van de EU IOA's. Tevens steunt het kabinet de doelen die met de verordening nagestreefd worden, zoals het moderniseren van de regelgeving voor informatiebeveiliging. Desalniettemin staat het kabinet kritisch tegenover enkele punten in het voorstel.

Het kabinet is geen voorstander van het behoud van eigen merkingen van EU IOA's. Het kabinet is van mening dat het niet wenselijk is dat er eigen (en extra) merkingen gehanteerd mogen worden door de EU IOA's, omdat dit leidt tot minder harmonisatie. Tevens is het kabinet van mening dat de, Council Security Rules (CSR)[14] die op dit moment herzien worden, de meest geavanceerde regelgeving voor de beveiliging van EUCI bevatten en als basis gebruikt dienen te worden voor deze verordening. De CSR zijn niet alleen het verst doorontwikkeld, maar ook opgesteld met instemming van de lidstaten en in de aanwezigheid van alle instellingen van de EU. Het kabinet zal bij de Commissie duidelijk maken dat er een groot draagvlak is voor de CSR en dat het logisch en efficient wordt geacht om hier gebruik van te maken als basis voor deze verordening.

Het kabinet staat kritisch tegenover de introductie van de categorie 'niet-gerubriceerde informatie'. Het kabinet acht de introductie van deze categorie informatie onwenselijk om drie redenen.

Ten eerste bestaat er in de lidstaten geen (juridisch) systeem voor de beveiliging van deze categorie informatie zoals dit voor EUCI is opgezet. Wanneer er EUCI gedeeld wordt met de lidstaten, geldt een wettelijk kader dat lidstaten met de EU zijn overeengekomen, waarbij alle partijen zich committeren aan het naleven van de vastgelegde beveiligingsmaatregelen voor EUCI.

[13] Overeenkomst tussen de lidstaten van de Europese Unie, in het kader van de Raad bijeen, betreffende de bescherming van in het belang van de Europese Unie uitgewisselde gerubriceerde informatie (2011/C 202/05).
[14] Besluit van de Raad van 23 september 2013 betreffende de beveiligingsvoorschriften voor de bescherming van gerubriceerde EU-informatie (2013/488/EU).

Tevens is er een systeem van toezicht en handhaving ingericht voor de naleving van de regelgeving. Voor de categorie 'niet-gerubriceerde informatie' is een dergelijk systeem niet ingericht. Indien informatie uit deze categorie gedeeld wordt met lidstaten bestaan er geen juridische en praktische voorzieningen om de informatiebeveiligingsregels voor deze categorie informatie na te leven. In het voorstel wordt beschreven dat bij het delen van informatie in deze categorie met lidstaten, zogenoemde 'verwerkingsinstructies' zullen worden bijgevoegd. De verantwoordelijkheid voor het opstellen van deze instructies zal bij de nader op te richten 'Subgroep inzake niet-gerubriceerde informatie' belegd worden. Het is op dit moment voor het kabinet onduidelijk waar de instructies uit zullen bestaan en in hoeverre deze praktisch uitvoerbaar zullen zijn. Tevens bestaat er geen wettelijke verplichting tot naleving van de genoemde verwerkingsinstructies door de lidstaten. De beveiliging van informatie in deze categorie is op deze manier dus niet gewaarborgd. Het is ook niet duidelijk hoe de beveiligingeisen voor deze categorie informatie zich verhouden tot de Wet openbaarheid van bestuur (Wob) en de Wet open overheid (Woo). Het kabinet zal de Commissie om verduidelijking vragen en haar zorgen delen m.b.t. de beveiliging van deze categorie informatie in de lidstaten.
Ten tweede leidt de verplichting tot het labelen van informatie in deze categorie tot een onwenselijke aanzienlijke toename in de administratieve lastendruk op de EU IOA's. Dit acht het kabinet onwenselijk.
Ten derde is het kabinet van mening dat de verschillen tussen de definities van de nieuwe categorie 'gevoelige niet-gerubriceerde informatie' en 'RESTREINT UE/EU-RESTRICTED' nihil zijn. Het kabinet benadrukt het belang van het voorkomen van duplicatie van regelgeving. Het kabinet acht dat bij correct gebruik van het reeds bestaande rubriceringssysteem de rubricering RESTREINT UE/EU-RESTRICTED volstaat.
Het kabinet is voorstander van het verwijderen van de gehele categorie 'niet-gerubriceerde informatie' uit de verordening. Een alternatief is het samenvoegen van de categorie 'gevoelige niet-gerubriceerde informatie' en de rubricering RESTREINT UE/EU-RESTRICTED onder de bestaande rubricering RESTREINT UE/EU-RESTRICTED. Het kabinet zal dit overbrengen aan de Commissie.

Wat betreft het gebruik van cryptografische producten voor de beveiliging van EUCI schrijft de verordening voor dat de Raad een lijst bijhoudt met goedgekeurde producten op basis van input van de nationale veiligheidsautoriteiten. Hierbij wordt niet gerefereerd aan het huidige systeem van Tweedelandsevaluaties[15]. Het kabinet hecht belang aan het behoud van het systeem van Tweedelandsevaluaties en de positie van de zogenoemde AQUA landen. De AQUA landen zijn een vijftal EU-lidstaten (waaronder Nederland) die op basis van hun expertise bevoegd zijn om Tweedelandsevaluaties uit te voeren. De Raad kan op basis van de Tweedelandsevaluaties cryptografische producten kwalificeren voor gebruik ten behoeve van de beveiliging van EUCI. Met dit systeem wordt gewaarborgd dat de EU cryptografische producten kan gebruiken waarbij door

[15] Een Tweedelandsevaluatie is een proces, werkwijze en normenkader dat binnen de EU is overeengekomen en wordt bewaakt door de AQUA Reference Group (ARG). Het doel is om ervoor te zorgen dat er een portfolio is met producten die gebruikt kunnen worden voor de bescherming van EUCI. Duisland, Zweden, Frankrijk, Italië en Nederland vormen de crypto evaluerende landen en leveren apparatuur en oplossingen voor EU IOA's voor de bescherming van spraak en data. De Tweedelandsevaluaties bieden waarborgen voor de kwaliteit van de beveiligingswaarde van het betreffende product (asssurance).

EU-lidstaten is vastgesteld dat zij een bepaald weerstandsniveau hebben. Dit draagt bij aan de autonomie en soevereiniteit van de Unie. In het voorstel worden eisen gesteld aan het gebruik van cryptografische producten. Het kabinet is van mening dat hierbij expliciet gerefereerd moet worden aan het systeem van Tweedelandsevaluaties. Het kabinet zal zich inzetten om het voorstel op dit punt aangepast te krijgen.

De verordening heeft als doel het verhogen van het niveau van informatiebeveiliging van de EU IOA's om zodoende informatie beter te beveiligen tegen de toenemende dreiging. Het kabinet acht sec deze verordening onvoldoende voor de weerbaarheid van de EU IOA's tegen de toenemende dreiging. Hoewel deze verordening wordt gezien als een stap in de goede richting, acht het kabinet aanvullende maatregelen nodig. Voorbeelden hiervan zijn het beter positioneren en het verbeteren van de slagkracht van de veiligheidsdirectoraten van de EU IOA's. Het kabinet zal hier aandacht voor vragen bij de Commissie. Het kabinet verwelkomt om die reden ook het voorstel tot de Verordening cybersecurity EU IOA's, dat parallel aan het voorliggende voorstel is gepresenteerd en waarover de Tweede Kamer een apart BNC-fiche ontvangt. Deze beoogt immers het niveau van cyberbeveiliging van de EU IOA's naar een hoger niveau te tillen en stelt daartoe concrete maatregelen voor.

De verwerking van persoonsgegevens die voortvloeit uit deze verordening, dient plaats te vinden in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG), richtlijn Gegevensbescherming, opsporing en vervolging[16] en met de grondrechten op eerbiediging van het privéleven en de bescherming van persoonsgegevens (resp. artikel 7 en 8 van het Handvest van de grondrechten van de Europese Unie). Het kabinet geeft nadrukkelijk aandacht aan de wijze waarop de voorstellen van de Commissie zich verhouden tot de genoemde wetgeving en jurisprudentie.

c) Eerste inschatting van krachtenveld

Een ruime meerderheid van de lidstaten erkent de noodzaak tot een hoger niveau van informatiebeveiliging in de EU IOA's. Ook is de meerderheid van de lidstaten voorstander van het harmoniseren van informatiebeveiligingsregels tot één gemeenschappelijke set van maatregelen. Het voorstel is reeds meerdere malen in de Council Security Committee besproken. Tijdens deze bijeenkomsten heeft een groot aantal lidstaten vraagtekens geplaatst bij de effectiviteit van de voorgestelde verordening met betrekking tot het harmoniseren van de regels. De inschatting van deze lidstaten is dat de voorgestelde verordening onvoldoende tot de gewenste harmonisering leidt omdat EU IOA's hun eigen interne regelgeving mogen behouden. Ook is een grote meerderheid van de lidstaten van mening dat er een scheiding gemaakt dient te worden tussen regelgeving voor EUCI en niet-gerubriceerde informatie en hiervoor separate verordeningen

[16] AVG is in NL geïmplementeerd in de WPG (https://wetten.overheid.nl/BWBR0022463/2020-01-01), Wjsg (https://wetten.overheid.nl/BWBR0014194/2020-01-01) en uitvoeringswet AVG (https://wetten.overheid.nl/BWBR0040940/2018-05-25). Verder relevant is de verordening voor instellingen die ook uitvoering geeft aan de AVG (https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32018R1725).edrij

opgesteld moeten worden. Verder is er een groot aantal lidstaten dat van mening is dat de herziene versie van de Council Security Rules (CSR) de basis zou moeten vormen van het voorstel voor gemeenschappelijke informatiebeveiligingsregels.

4. Beoordeling bevoegdheid, subsidiariteit en proportionaliteit

a) *Bevoegdheid*

Het oordeel van het kabinet ten aanzien van de bevoegdheid is positief. Het voorstel is gebaseerd op artikel 298 VWEU en artikel 106bis Euratom-verdrag. Artikel 298, eerste lid, VWEU bepaalt dat de EU IOA's bij de vervulling van hun taken steunen op een open, doeltreffend en onafhankelijk Europees ambtenarenapparaat. Artikel 298, tweede lid, VWEU geeft de EU de bevoegdheid, met inachtneming van het statuut en de regeling vastgesteld op grond van artikel 336 VWEU bepalingen daartoe vast te stellen. In artikel 106bis Euratom-verdrag wordt artikel 298 VWEU van toepassing verklaard op het Euratom-verdrag. Het kabinet kan zich vinden in de rechtsgrondslag.

Aangezien het voorstel in hoofdzaak ziet op het treffen van maatregelen ten behoeve van de informatiebeveiliging in de EU IOA's, wat buiten de in de artikelen 3 en 6 VWEU bedoelde artikelen valt, is sprake van een gedeelde bevoegdheid van de EU en de lidstaten (artikel 4, eerste lid, VWEU).

b) Subsidiariteit

Het oordeel van het kabinet is positief. De verordening heeft tot doel een hoog niveau van informatiebeveiliging voor de EU IOA's te bereiken. Aangezien het gaat om regels voor de EU-instellingen, ligt het voor de hand dat dit op EU-niveau geregeld wordt. Dit zou niet door de lidstaten kunnen worden verwezenlijkt. Optreden op EU-niveau is daarom gerechtvaardigd.

c) Proportionaliteit

Het oordeel van het kabinet is positief, met kanttekening. De verordening heeft tot doel het verhogen van het gemeenschappelijke niveau van informatiebeveiliging van de EU IOA's door de regelgeving te harmoniseren, moderniseren en onderlinge samenwerking te bevorderen. Het voorgestelde optreden is geschikt om deze doelstelling te bereiken, omdat de verordening leidt tot een verbetering van uniformiteit en eenduidigheid in de informatiebeveiligingsregels voor de EU IOA's. Tevens worden de regels gemoderniseerd en wordt rekening gehouden met nieuwe technologieën en de praktijk van het thuiswerken. Echter staat het kabinet kritisch tegenover de introductie van de categorie 'niet-gerubriceerde informatie' en met name 'gevoelige niet-gerubriceerde informatie'. De introductie van deze categorie zorgt voor een toename in de administratieve lastendruk voor de EU IOA's. Tevens bestaan er geen juridische en praktische voorzieningen om de informatiebeveiligingsregels voor deze categorie informatie na te leven indien deze informatie gedeeld wordt met de lidstaten. Het kabinet is van mening dat het introduceren van deze categorie verder gaat dan noodzakelijk, omdat de reeds bestaande rubricering 'RESTREINT UE/EU-RESTRICTED' geschikt is voor het beveiligen van deze categorie informatie.

5. Financiële consequenties, gevolgen voor regeldruk, concurrentiekracht en geopolitieke aspecten

a) Consequenties EU-begroting

Volgens de Commissie kunnen de kosten voor de implementatie van de voorgestelde verordening gedekt worden uit de budgetten van de bestaande programma's ter verbetering van informatiebeveiliging. De verwachte kosten voor personele middelen bedragen 0.314 miljoen per jaar voor de periode 2023-2027, te financieren onder rubriek 7 van het meerjarig financieel kader. Ten behoeve van het realiseren van het secretariaat voor het informatiebeveiligingscomité is volgens de Commissie een uitbreiding van 2 FTE vereist. Andere administratieve uitgaven zijn niet voorzien. Het is lastig in te schatten of het beschikbaar gestelde budget voldoende is om de beoogde doelen te bereiken. Het kabinet is van mening dat eventuele EU-middelen gevonden dienen te worden binnen de in de Raad afgesproken financiële kaders van de EU-begroting 2021-2027 en dat deze moeten passen bij een prudente ontwikkeling van de jaarbegroting. Daarnaast moet de ontwikkeling van de administratieve uitgaven in lijn zijn met de ER-conclusies van juli 2020 over het MFK-akkoord. Het kabinet is kritisch over de stijging van het aantal werknemers, maar ziet daar in dit geval de noodzaak van in. Het kabinet benadrukt het belang van voldoende budget voor de adequate implementatie van de verordening en zal dit onder de aandacht brengen bij de Commissie.

b) Financiële consequenties (incl. personele) voor Rijksoverheid en/ of medeoverheden

Volgens het impact assessment van de Commissie heeft het voorstel nauwelijks tot geen implicaties voor de lidstaten. Het kabinet kan zich niet vinden in deze analyse. Het kabinet schat in dat de verordening door de introductie van de categorie 'niet-gerubriceerde informatie' wel degelijk gevolgen voor de lidstaten zal hebben. Wanneer informatie uit deze categorie gedeeld wordt met ministeries en bedrijven in de lidstaten zullen er verwerkingsinstructies worden bijgevoegd. Bedrijven en ministeries zullen worden geacht zich hieraan te houden. Het is op dit moment niet duidelijk hoe de verwerkingsinstructies in de praktijk zullen worden vormgegeven. Het kabinet verwacht dat de naleving ervan echter wel impact op bedrijven en ministeries zal hebben. Het kabinet zal de Commissie vragen om een nadere toelichting op de verwerkingsinstructies en hoe het toezicht op de naleving hiervan wordt ingericht. (Eventuele) budgettaire gevolgen worden ingepast op de begroting van het/de beleidsverantwoordelijk (e) departement(en), conform de regels van de budgetdiscipline.

c) Financiële consequenties en gevolgen voor regeldruk voor bedrijfsleven en burger

Volgens de impact assessment van de Commissie heeft de verordening geen significante financiële gevolgen voor het bedrijfsleven. Het kabinet betwijfelt dit vanwege de introductie van beveiligingsregels voor de informatie in de categorie 'niet-gerubriceerde informatie'. Het komt regelmatig voor dat de Commissie producten en diensten van Nederlandse bedrijven afneemt die die daarvoor in aanraking komen met informatie van de Commissie. Hierbij zijn zij contractueel gebonden aan de eisen die de Commissie stelt, waaronder het beveiligen van informatie. Voor wat betreft de verwerking en opslag van EUCI hebben de desbetreffende bedrijven reeds materieel aangeschaft en procedures ingericht om de geldende regelgeving voor informatiebeveiliging na te

leven. Tevens is er een systeem van toezicht ingericht waarbij de Nederlandse Nationale Veiligheidsautoriteit (NSA) de bedrijven inspecteert en controleert of zij aan alle vereisten voldoen om EUCI te mogen verwerken en opslaan. Voor de nieuwe categorie 'niet-gerubriceerde informatie' bestaat dit niet. Uit de verordening blijkt dat wanneer de Commissie informatie uit deze categorie deelt met bedrijven, zij zogenoemde verwerkingsinstructies bijvoegt waar de bedrijven zich aan dienen te houden. Het ligt in de lijn der verwachting dat bedrijven moeten investeren (bijvoorbeeld in cryptomiddelen) om deze instructies uit te kunnen voeren en zo aan de verplichtingen als gevolg van de voorgestelde verordening te voldoen. De exacte financiële consequenties hiervan voor het bedrijfsleven zijn nog onduidelijk. Het valt niet uit te sluiten dat eventuele kosten als gevolg van de vereiste investeringen in informatiebeveiliging worden doorgerekend aan burgers middels een prijsstijging voor een product en/of dienst.

d) Gevolgen voor concurrentiekracht en geopolitieke aspecten

De verordening heeft geen gevolgen voor de regeldruk of concurrentiekracht. Ten aanzien van geopolitieke aspecten geldt dat een hoger niveau van informatiebeveiliging (digitale) spionageactiviteiten door statelijke actoren bemoeilijkt en bijdraagt aan het voorkomen van incidenten waarbij informatie gecompromitteerd raakt. Derhalve kan de voorgestelde verordening bijdragen aan het versterken van de weerbaarheid van de EU en de bescherming van EU-belangen. Tevens draagt een hoger niveau van informatiebeveiliging bij aan het borgen van de strategische positie van de EU in het mondiale speelveld en versterkt het de positie van de EU in internationale onderhandelingen. Verder verbetert de positie van de EU als samenwerkingspartner, omdat als gevolg van de eenduidigheid in regelgeving het uitwisselen van informatie met de EU makkelijker wordt.

6. Implicaties juridisch

a) Consequenties voor nationale en decentrale regelgeving en/of sanctionering beleid (inclusief toepassing van de lex silencio positivo)

Er worden geen consequenties verwacht voor nationale en decentrale regelgeving en/of sanctionering beleid.

b) Gedelegeerde en/of uitvoeringshandelingen, incl. NL-beoordeling daarvan

Niet van toepassing

c) Voorgestelde implementatietermijn (bij richtlijnen), dan wel voorgestelde datum inwerkingtreding (bij verordeningen en besluiten) met commentaar t.a.v. haalbaarheid

De verordening treedt in werking op de twintigste dag na publicatie in het Publicatieblad van de Europese Unie. De verordening is van toepassing vanaf twee jaar na deze datum. Gezien de urgentie van de geschetste problematiek zal het kabinet aandringen op spoedige inwerkingtreding.

d) Wenselijkheid evaluatie-/horizonbepaling

Uiterlijk drie jaar na de toepassingsdatum van de verordening zal de Commissie een rapportage over de implementatie presenteren aan het Europees Parlement en de Raad. De Commissie stelt

voor om vijf jaar na de toepassing van de verordening een evaluatie uit te voeren. De Commissie zal de uitkomsten rapporteren aan het Europees Parlement en de Raad. Het kabinet onderschrijft het belang van een evaluatie en staat hier positief tegenover.

e) Constitutionele toets
Niet van toepassing

7. Implicaties voor uitvoering en/of handhaving
De verantwoordelijkheid voor de uitvoering van de verordening ligt primair bij de EU IOA's. Hoewel de situatie per EU IOA verschilt staat het kabinet positief tegen de uitvoerbaarheid van het voorstel. Het kabinet verwacht dat de voorgestelde verordening zal leiden tot een verbetering in de uitvoerbaarheid van de regelgeving voor de beveiliging van EUCI omdat de verordening harmonisering tot doel heeft. Het harmoniseren van verschillende soorten regelgeving voor de beveiliging van EUCI leidt tot overzichtelijkheid en eenduidigheid en komt de uitvoerbaarheid ten goede.

Wat betreft de categorie 'niet-gerubriceerde informatie' is de uitvoerbaarheid lastig in te schatten. De verplichting om alle informatie in deze categorie te labelen en extra beveiligingsmaatregelen te treffen bij verwerking en opslag van informatie uit deze categorie leidt tot een toename in de administratieve lastendruk bij zowel de EU IOA's als de bedrijven en ministeries in lidstaten.

De verordening schrijft voor dat de nader op te richten coördinatiegroep wordt bijgestaan en geadviseerd door een comité voor informatiebeveiliging. Dit comité zal bestaan uit vertegenwoordigers van de NSA van elke lidstaat. Het kabinet staat positief tegenover de uitvoerbaarheid hiervan.

Aangaande de beveiliging van EUCI speelt de NSA een rol in de handhaving in Nederland. De NSA houdt toezicht op de beveiliging van EUCI in Nederland en verstrekt *personnel security clearances*. Ook voert de NSA inspecties uit bij bedrijven en ministeries die EUCI verwerken en opslaan, en is betrokken bij de *security assessment visits* die op Nederlands grondgebied plaatsvinden. Indien deze rol in de huidige vorm blijft bestaan, en dus alleen geldt ten behoeve van de beveiliging van EUCI, zal er naar verwachting geen sprake zijn van een taakverzwaring. Mocht de autoriteitsrol van de NSA uitgebreid worden naar de categorie 'niet-gerubriceerde informatie', dan leidt dit wel tot taakverzwaring, omdat de NSA tot op heden geen bevoegdheid heeft voor het houden van toezicht op 'niet-gerubriceerde informatie'. In het huidige voorstel is een uitbreiding van de NSA-rol niet voorzien. Dit betekent dat er geen centrale verantwoordelijke autoriteit is in Nederland die toezicht houdt op het naleven van de beveiliginsregels voor 'niet-gerubriceerde informatie'. Tevens is niet duidelijk hoe de beveiliging van informatie in de categorie 'gevoelige niet-gerubriceerde informatie' zich verhoudt tot de Wob en de Woo. Het kabinet zal dit onder de aandacht brengen bij de Commissie en om verduidelijking vragen.

8. Implicaties voor ontwikkelingslanden

Geen implicaties voor ontwikkelingslanden.