Ministerie van Economische Zaken en Klimaat

Nota bevat informatie die niet openbaar gemaakt kan worden:
☒ NEE ☐ JA, ONDER BETREFFEND KOPJE ☐ JA, VERSPREID OVER NOTA (MARKEER) ☐ JA, GEHEEL

Aan de Staatssecretaris EZK

Directie Wetgeving en Juridische Zaken

Auteur
[redacted]

Datum
1 juli 2021

Kenmerk
WJZ / 21176932

Kopie aan

Bijlage(n)

Beslisnota

Beslisnota nota naar aanleiding van het verslag Uitvoeringswetwet cyberbeveiligingsverordening

Aanleiding

Op 15 juni 2021 heeft de vaste commissie voor Economische Zaken en Klimaat het verslag inzake de Uitvoeringswet cyberbeveiligingsverordening (hierna: het wetsvoorstel) uitgebracht (Kamerstuk 35838). In dit verslag hebben Kamerleden (VVD, D66, CDA, SP, GroenLinks, ChristenUnie) vragen over het wetsvoorstel gesteld. U reageert op het verslag met bijgaande nota naar aanleiding van het verslag.

Geadviseerd besluit

U kunt de volgende stukken ondertekenen:
1. De aanbiedingsbrief aan de Tweede Kamer;
2. De nota naar aanleiding van het verslag.

Kernpunten

- De belangrijkste onderwerpen waar vragen over worden gesteld in het verslag van de TK en die worden beantwoord in de nota naar aanleiding ervan zijn:
    - het al dan niet verplichten van certificering, en eventuele nationale maatregelen hiervoor;
    - de wisselwerking met nationale cyberbeveiligingscertificeringsregelingen;
    - de aanwijzing van Agentschap Telecom als nationale cyberbeveiligingscertificeringsautoriteit;
    - de regels omtrent patches, hacks en updates;
    - conformiteitsbeoordelingsinstanties;
    - de regeldruk.

- In antwoord op de gestelde vragen geeft u aan dat:
    - de regering zich conform de motie Paternotte c.s. blijft inzetten voor verplichte cybersecuritycertificering op Europees niveau[1];
    - een nationale certificeringsregeling wordt ingetrokken op het moment dan een Europese cyberbeveiligingscertificeringsregeling voor hetzelfde onderwerp in werking treedt en dat de regering zich ervoor zal inzetten om de transitie op goede wijze te laten verlopen;
    - voor AT als nationale cyberbeveiligingscertificeringsautoriteit is gekozen omdat AT zich bezighoudt met zowel toezichthoudende als uitvoerende werkzaamheden binnen het brede digitale domein, en ervaring heeft met cybersecurityvraagstukken;
    - de regels omtrent patches, hacks en updates in elke Europese cyberbeveiligingscertificeringsregeling zullen worden opgenomen en dat bij de uitwerking van specifieke Europese cyberbeveiligingscertificeringsregelingen de regering erop zal toezien dat deze voldoende zijn;
    - de onafhankelijkheid van conformiteitbeoordelingsinstanties een kernvoorwaarde van de accreditatie is en gaat u in op een aantal aspecten rondom conformiteitsbeoordelingsinstanties en accreditatie (bijvoorbeeld met betrekking tot organisaties uit derde landen);
    - wanneer een Europese cyberbeveiligingscertificeringsregeling is vastgesteld, inzicht kan worden gegeven in de daaruit voortvloeiende regeldruk en kosten.

[1] Kamerstuk 21 501-30, nr. 422.