

Aan de Staatssecretaris van Economische Zaken - Digitale Economie en
Soevereiniteit

Directoraat-generaal
Economie en Digitalisering
Directie Digitale Economie

Auteur

Datum aangemaakt
2 oktober 2026

Kenmerk
DGED-DE / 108487934

Kopie aan

Bijlage(n)
1

nota

TER BESLISSING

Beantwoording Kamervragen D66 & CDA: "AI-
modellen die buiten hun testomgeving inbreken
bij organisaties"

Aanleiding

De leden El Boujdaini (D66) en Zwinkels (CDA) hebben schriftelijke vragen gesteld aan de Staatssecretaris van Economische Zaken en Klimaat over AI-modellen die buiten hun testomgeving inbreken bij organisaties.

Advies

U kunt akkoord gaan met verzending van bijgevoegde beantwoording naar de Tweede Kamer.

Kernpunten

- De leden El Boujdaini (D66) en Zwinkels (CDA) hebben meerdere schriftelijke vragen gesteld naar aanleiding van nieuwsberichten over AI-modellen die buiten hun testomgeving inbreken bij organisaties.
- De vragen behandelen, in de kern, de verantwoordelijkheidsvraag voor veilige AI testomgevingen.
- Tevens wordt gevraagd of er aanvullende maatregelen, standaarden of andere activiteiten worden ondernomen om toekomstige uitbraak van AI agenten te voorkomen.

Ontvangen BPZ