Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2025–2026

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

873

Vragen van de leden **Boswijk**, **Jumelet** (beiden CDA), **Peter de Groot**, **Van der Burg** (beiden VVD), **Grinwis** (ChristenUnie), **Paternotte** en **Klos** (beiden D66) aan de Ministers van Buitenlandse Zaken en van Klimaat en Groene Groei over *het artikel «Woede om miljoenenorder: vier miljoen slimme meters komen straks uit China»* (ingezonden 31 december 2025).

Antwoord van Minister **Hermans** (Klimaat en Groene Groei) (ontvangen 14 januari 2026).

Vraag 1
Bent u bekend met de berichtgeving dat netbeheerders circa vier miljoen slimme meters gaan inkopen bij Chinese leveranciers? Zo ja, wat is uw oordeel hierover?[1]

Antwoord 1
Ja, ik ben bekend met deze berichtgeving. De berichtgeving gaat over de meetmodule, een onderdeel van de slimme meter dat alleen het elektriciteitsverbruik op digitale wijze meet. Deze meetmodule introduceert daarmee geen risico voor de leveringszekerheid van energie.
De verzending en de versleuteling van data naar de netbeheerders en de communicatie met andere apparaten loopt niet via deze meetmodule. De meetmodule bevat ook geen schakelaar en kan niet op afstand worden uitgeschakeld waardoor er geen effect is op de beschikbaarheid van energie. De leveranciers van het betreffende onderdeel en andere niet-geautoriseerde partijen kunnen niet meelezen met de data van de nieuwe generatie slimme meter. De veiligheid van de data wordt door de netbeheerders gewaarborgd door middel van encryptie en autorisaties. In de beantwoording van vraag 7, 8, 9 en 10 wordt dataveiligheid nader verdiept. Het kabinet is tegen deze achtergrond van oordeel dat de betreffende inkoop geen ontoelaatbaar risico vormt voor Nederlandse consumenten.

Vraag 2 en 3
Welke afwegingen zijn gemaakt over de economische afhankelijkheid van China bij de keuze voor deze leveranciers?
Is onderzocht of voldoende capaciteit bestaat bij Europese of Nederlandse producenten om deze meters te leveren? Zo ja, wat zijn de uitkomsten?

[1] Telegraaf van 30 december 2025

ah-tk-20252026-873
ISSN 0921 - 7398
's-Gravenhage 2026

Antwoord 2 en 3
Betrouwbare waardeketens voor vitale energie-infrastructuur zijn essentieel voor het waarborgen van de leveringszekerheid en onze nationale veiligheid. Leveringszekerheid in de product waardeketen is één van de onderdelen van de risicoanalyse die is uitgevoerd door de netbeheerders. Om risico's ten aanzien van de leveringszekerheid te mitigeren, is onder andere besloten voor elke hardware component in de slimme meter voor twee verschillende leveranciers te kiezen. Eén van de twee leveranciers dient afkomstig te zijn uit een land dat partij is bij de multilaterale Overeenkomst inzake overheidsopdrachten (Government Procurement Agreement – GPA). Deze overeenkomst beoogt wederzijdse openstelling van overheidsopdrachten tussen deelnemende landen op basis van transparantie, non-discriminatie en rechtszekerheid. De Europese Unie onderhoudt met deze GPA-partijen structurele en wederkerige handelsrelaties die zijn gebaseerd op internationale afspraken, hetgeen bijdraagt aan een betrouwbare samenwerking binnen de publieke aanbestedingen.
In dit geval betekent dit dat de meetmodule die Kaifa Technology levert, ook wordt geleverd door het Franse Sagemcom. Indien noodzakelijk kunnen de netbeheerders een beroep doen op de Franse leverancier om alle leveringen over te nemen en de dienstverlening te continueren. Dit houdt in dat, indien één van de partijen niet in staat is om te leveren, de andere partij over voldoende capaciteit beschikt om de levering tot 100% te continueren. Hierdoor is de leveringszekerheid van dit onderdeel geborgd. Voor dit leveranciersmodel is ook gekozen om de Europese productie van meetmodules te versterken en beschikbaar te houden.
Voor de verschillende onderdelen van het systeem is een uitgebreide marktconsultatie gedaan. Voor de componenten die niet als risicovol beschouwd zijn, is gekozen voor maximale concurrentie om de maatschappelijke kosten zo laag mogelijk te houden.

Vraag 4, 5 en 6
Welke risicoanalyses zijn uitgevoerd met betrekking tot nationale veiligheid en cybersecurity bij het gebruik van slimme meters, die geproduceerd zijn door bedrijven gevestigd in China?
Zijn er specifieke dreigingsanalyses voor mogelijke beïnvloeding van het energiesysteem (bijvoorbeeld verbruikscijfers manipuleren of storingen veroorzaken) wanneer apparaten in handen zijn van derde landen met potentiële tegenstellingen?
Hebben de AIVD, MIVD of NCTV hierover advies uitgebracht richting het kabinet of netbeheerders? Kunt u die adviezen openbaar maken of samenvatten?

Antwoord 4, 5 en 6
De netbeheerders hebben een risicoanalyse en onderzoek uitgevoerd. Hierbij is gebruik gemaakt van verschillende analyses, waaronder het Dreigingsbeeld Statelijke Actoren (DBSA) en het Cybersecuritybeeld Nederland, beide gepubliceerd door de NCTV. Daarnaast hebben de netbeheerders de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) bevraagd over risico's in dit aanbestedingstraject. In overleg met de netbeheerders en het Ministerie van Klimaat en Groene Groei heeft de AIVD in algemene zin het dreigingsbeeld, conform bovengenoemde analyses, geschetst op het concept van de nieuwe generatie slimme meter. Mede op basis van deze informatie hebben de netbeheerders maatregelen toegepast waarmee er geen ontoelaatbaar risico is.
De slimme meter is modulair ontworpen en voor de afzonderlijke componenten is een risicobeoordeling opgesteld. De beschikbare analyses en informatie zijn bij het opstellen van deze risicobeoordelingen meegenomen. De risicobeoordeling heeft geresulteerd in mitigerende maatregelen, waaronder die ten aanzien van productleveringszekerheid en dataveiligheid. Er is dus vooraf rekening gehouden met mogelijke risico's voor bijvoorbeeld de energie- en productleveringszekerheid en de dataveiligheid van consumenten bij het vormgeven van de aanbesteding.
Daarnaast zijn de netbeheerders gehouden aan de nationale en Europese aanbestedingsregels. Ter verdere bevordering van de bescherming van vitale processen in de energiesector zijn in de nieuwe Energiewet – die sinds 1 januari van kracht is – regels opgenomen voor de bescherming van deze

processen. Deze regels worden momenteel nader uitgewerkt in onderliggende regelgeving.

Vraag 7, 8 en 9
Welke data worden precies verzameld door deze slimme meters en op welke frequentie (bijvoorbeeld per minuut, per uur)?
Wordt er onderscheid gemaakt tussen noodzakelijke data voor het energienetbeheer en privacygevoelige data? Zo ja, hoe worden die gescheiden?
Welke maatregelen zijn getroffen om te waarborgen dat gegevensuitwisseling volledig conform de Algemene verordening gegevensbescherming (AVG) en EU-privacyregels verloopt?

Antwoord 7, 8 en 9
De netbeheerders houden zich aan de wettelijke voorschriften omtrent databeheer en privacy en zijn op grond van de Energiewet[2] verplicht hun gegevens te beveiligen en te beschermen. De huidige circa 8 miljoen slimme meters voldoen aan de gestelde (technische) eisen in het Besluit op afstand uitleesbare meetinrichtingen (BOAUM), die gelden onder de Energiewet.[3] Ook bij de nieuwe generatie slimme meter geven de netbeheerders uitvoering aan de eisen uit het BOAUM. In deze eisen is onder meer vereist dat de meters zodanig beveiligd zijn tegen fraude met, misbruik van of inbreuk op de meters dat een passend beveiligingsniveau is gegarandeerd. Hierbij moet rekening gehouden worden met de internationale stand van de techniek en de uitvoeringskosten.
Conform het BOAUM registreert de meter het actuele vermogen (in Watt) en per kwartier de meterstand. De netbeheerders lezen de meters maximaal één keer per dag uit, vaak in de nacht. De netbeheerder leest enkel datgene uit wat noodzakelijk is voor het functioneren van het elektriciteitssysteem in den brede, wat ook is vastgelegd in de Energiewet en onderliggende regelgeving. Onder de Energiewet[4] is de netbeheerder bevoegd per aansluiting de kwartierstanden uit te lezen ten behoeve van de onbalansverrekening als onderdeel van de balanceringstaak van TenneT.
Naast het regime van de Energiewet geldt, voor zover het gaat om persoonsgegevens, ook de Algemene verordening gegevensbescherming (AVG). Bij elke verwerking van persoonsgegevens geldt voor de netbeheerders dat deze verwerking rechtmatig moet zijn in het licht van de voorwaarden in artikel 6 AVG. Ten aanzien van de omgang met slimme meterdata voor de uitvoering van hun wettelijke taken hebben de netbeheerders de «Gedragscode Slim Netbeheer» opgesteld die in februari 2022 door de Autoriteit Persoonsgegevens is goedgekeurd.[5]

Vraag 10
Welke technische safeguards zijn ingebouwd om te voorkomen dat externe (buitenlandse) fabrikanten of andere externe partijen toegang krijgen tot het backend-systeem waarmee meters data uitwisselen?

Antwoord 10
Zoals hiervoor opgemerkt gelden voor de netbeheerders verplichtingen ten aanzien van gegevensbescherming en -beveiliging. Voor het uitlezen van de nieuwe generatie slimme meters wordt door de netbeheerders een centraal systeem opgezet. De netbeheerders ontwikkelen dit systeem zelf en maken daarbij geen gebruik van buitenlandse fabrikanten, om de veiligheid van de data te waarborgen. De veiligheid van de data wordt door de netbeheerders gewaarborgd door middel van encryptie.

Vraag 11
Is er nog een mogelijkheid dat de Rijksoverheid ingrijpt en deze aanbesteding terugdraait, indien blijkt dat de veiligheid teveel in het geding komt?

---

[2] Energiewet artikel 4.2.
[3] Op grond van de overgangsregeling in artikel 7.52 Energiewet blijven de relevante eisen uit artikel 4 van het BOAUM vanaf 1 januari 2026 nog van kracht.
[4] Zie met name artikel 3.49.
[5] Autoriteit Persoonsgegevens, «Besluit inzake de verklaring omtrent gedragscode Slim Netbeheer van Vereniging Netbeheer Nederland; z2021-00382», Staatscourant 2022, nr. 11739.

Antwoord 11
Het waarborgen van productleveringszekerheid en nationale veiligheid is voor het kabinet van groot belang. De beoordeling van de netbeheerders dat de meetmodule een laag risicoprofiel kent, in combinatie met de genomen mitigerende maatregelen passend bij dit risicoprofiel, resulteert erin dat het kabinet vanuit veiligheidsoverwegingen op dit moment geen reden ziet om in te grijpen bij deze aanbesteding. Indien het kabinet in de toekomst risico's vaststelt voor de nationale veiligheid of leveringszekerheid zal het maatregelen treffen om een dergelijk risico te mitigeren.