

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

1947

Vragen van het lid **Inge van Dijk** (CDA) aan de Minister van Financiën over *het bericht: «Fiserv neemt CCV over» van 19 maart* (ingezonden 26 maart 2025).

Antwoord van Minister **Heinen** (Financiën) (ontvangen 14 april 2025)

Vraag 1

Heeft u kennisgenomen van de aangekondigde overname van CCV, aanbieder van betaaloplossingen aan zo'n 600.000 bedrijven in Nederland, België en Duitsland, door Fiserv, Inc., een Amerikaanse aanbieder van technologie voor betalingen en financiële dienstverlening?¹

Antwoord 1

Ja.

Vraag 2

Klopt het dat bijna elke retailbetaling in Nederland via CCV loopt?

Antwoord 2

Nee, dat klopt niet. CCV is samen met vele andere partijen actief op de markt voor retailbetalingen. CCV is één van de grotere aanbieders van betaalautomaten aan de kassa en bijbehorende (betaal)diensten aan winkeliers en horecaondernemers in Nederland, maar retailbetalingen lopen ook via andere partijen. CCV heeft een vergunning bij De Nederlandsche Bank als afwikkelonderneming en als betaaldienstverleners.

Vraag 3

Bent u van mening dat CCV tot de kritieke betalingsinfrastructuur van Nederland behoort?

Antwoord 3

Welke instellingen wel en niet tot de kritieke (betalings)infrastructuur behoren heb ik samen met de Minister van Justitie en veiligheid en in samenspraak met de toezichthouders bepaald. Ik kan geen openbare uitspraken doen over

¹ https://www.ccv.eu/nl/over-ccv/nieuws/pers-en-media/fiserv-neemt-ccv-over?srsId=AfmBOowcLx1AcaDNqHpmm0lCbyjqInrQU8A_9-vFq-LKSdq1UKdPzM3

welke instellingen onder de kritieke, dan wel vitale, infrastructuur van Nederland behoren aangezien dit vertrouwelijke informatie betreft. Wel is het zo dat investeringen in vitale aanbieders die binnen de reikwijdte van de Wet veiligheidstoets investeringen, fusies en overnames (Wet vifo) vallen, moeten worden gemeld en worden beoordeeld op risico's voor de nationale veiligheid. Omdat dit ook vertrouwelijke informatie betreft kan ik niet ingaan op berichten in de media of iets wel of niet is gemeld, en kan ik geen informatie delen over de uitkomsten van een eventueel onderzoek.

Vraag 4

Klopt het dat bedrijven in de VS onder de «Cloud Act» gedwongen kunnen worden om data over betalingen af te staan, wat beïnvloeding van de dienstverlening mogelijk maakt?

Antwoord 4

De Clarifying Lawful Use of Overseas Data Act (CLOUD Act) is per maart 2018 van toepassing in de Verenigde Staten. Aanbieders van elektronische communicatiediensten (ECD's) of *remote computing services* (RCS) worden, indien aan de wettelijke voorwaarden hiervoor wordt voldaan, verplicht om gegevens die middels hun diensten worden verstuurd te bewaren en te verstrekken op verzoek van de Amerikaanse overheid. Of een bedrijf dat buiten de VS is gevestigd is onder de werking van de CLOUD Act valt, is afhankelijk van het soort bevel dat op grond van die wet wordt uitgevaardigd en van de concrete feiten en omstandigheden van de casus.

Vraag 5

Zou het na de overname kunnen voorkomen dat onder de Cloud Act ook het afstaan van data van betalingen via CCV, dus van onder andere de Nederlandse markt, kan worden afgedwongen?

Antwoord 5

CCV, dat zelf niet in de VS is gevestigd, zou onder de werking van de Amerikaanse CLOUD Act kunnen vallen na de overname. Hiervoor gelden echter verschillende voorwaarden. Zo moet deze entiteit zodanige banden met de Verenigde Staten hebben dat een Amerikaanse rechter (persoonlijke) jurisdictie over haar heeft. Daarnaast is een bevel nodig van de Amerikaanse overheid dat aannemelijk maakt dat er een gegronde verdenking bestaat dat de gezochte communicatie daadwerkelijk bewijs zal opleveren van een strafbaar feit. Daarnaast moet de EU-entiteit het gevraagde gegevensmateriaal in bezit, bewaring of onder controle hebben om onder het bevel te vallen.² Mocht deze casus onder de CLOUD Act vallen, dan dient opgemerkt te worden dat het risico dat de Amerikaanse overheid toegang krijgt tot de gegevens in de praktijk klein is. Het Nationaal Cyber Security Centrum (NCSC) heeft in 2022 een algemene juridische analyse laten uitvoeren naar de mogelijke impact van de CLOUD act op diverse cloud providers. Hieruit blijkt dat de risico's beperkt lijken te zijn.³

Vraag 6

Zo ja, kunt u inzichtelijk maken wat hiervan de mogelijke gevolgen zijn en of dit wenselijk is?

Antwoord 6

In algemene zin kan toegang tot Europese betaalgegevens door een buitenlandse overheid leiden tot risico's op het gebied van privacy, gegevensbescherming en het vertrouwen van klanten in financiële instellingen. Hoewel de kans dat dergelijke toegang zich in de praktijk voordoet als relatief laag wordt ingeschat, gezien de voorwaarden die geschetst worden in het antwoord op vraag 5, kan dit risico niet volledig worden uitgesloten. Wel kent

² Zie voor een meer gedetailleerde omschrijving voor de juridische voorwaarden voor een verzoek onder de Cloud Act het memo van Greenberg Traurig geschreven in opdracht van het NCSC: Cloud Act Memo | Publicatie | Nationaal Cyber Security Centrum.

³ <https://english.ncsc.nl/publications/reports/2022/november/23/cloud-act-requests>

de Europese Unie regelgeving die deze risico's beperkt, zie antwoord op vraag 7.

Vraag 7

Is er Nederlandse of Europese (privacy-)regelgeving die deze data beschermt?

Antwoord 7

Ja, de Europese Algemene verordening gegevensbescherming (AVG) is sinds 25 mei 2018 van toepassing in de gehele Europese Unie. De AVG is het normenkader voor de bescherming van persoonsgegevens, inclusief de doorgifte van gegevens naar landen buiten de Europese Economische Ruimte, zogenaamde «derde landen». Betaaldata vallen hier ook onder. Europese bedrijven kunnen geraakt worden door de extraterritoriale werking van buitenlandse wetgeving zoals de CLOUD Act waarbij ze moeten voldoen aan zowel Amerikaanse als Europese regelgeving. Hoewel de AVG dus een sterke bescherming biedt, is het belangrijk voor Europese bedrijven om zich bewust te zijn van de mogelijke impact van de CLOUD Act en passende maatregelen te nemen om de hoge normen uit de AVG te waarborgen. De meeste Amerikaanse aanbieders van ECD's hebben zelf ook passende maatregelen genomen om persoonsgegevens te beschermen om te kunnen voldoen aan de AVG en specifiek de Europese normen omtrent doorgifte van persoonsgegevens naar derde landen. Met standaard contractbepalingen van de Europese Commissie kunnen hierover afspraken worden gemaakt. Daarnaast bestaat er tussen de EU en de Verenigde Staten het EU-US Data Privacy Framework waarin de Europese Commissie en de Amerikaanse regering onder meer afspraken hebben gemaakt over de rechtsbescherming van EU-burgers wanneer gegevens worden doorgegeven aan de VS. Tot slot passen Amerikaanse ECD's technische maatregelen, zoals encryptie, toe om gegevens af te schermen.