Autoriteit Financiële Markten

De AFM doet geen mededelingen over de keuzes die worden gemaakt in de bedrijfsvoering.

Tweede Kamer

Waarom besloot het bestuur van de Tweede Kamer om zijn infrastructuur onder te brengen bij Microsoft?
De Tweede Kamer is een te kleine organisatie om zelf een e-maildienst te ontwikkelen en onderhouden. Dat zou bovendien de nodige veiligheids- en continuiteitsrisico's met zich meebrengen. Daarom is – na zorgvuldige afweging – gekozen voor een gerenommeerde partij, die garant kan staan voor een betrouwbare dienstverlening.

Is de aard van de communicatie binnen de Tweede Kamer te rijmen met het feit dat de Amerikaanse inlichtingendiensten het wettelijk recht hebben om die informatie op te vragen, ook al staat de informatie fysiek in Nederland?
De Tweede Kamer heeft een zorgvuldige afweging gemaakt en volgt hierin het Rijkscloud beleid. Daarnaast is het staand beleid dat er bij de Tweede Kamer geen geheime informatie via de cloud wordt gedeeld.

Is gebruik van een Nederlandse cloudprovider overwogen?
Nee, niet door de Tweede Kamer. Ook hier volgen wij het Rijkscloud beleid en de aanbestedingen en contracten die daaruit zijn voortgekomen. We volgen de ontwikkelingen rond een Europese cloud (zoals GaiaX) nauwgezet.

Eerste Kamer

Er zijn Nederlandse leveranciers overwogen, maar Microsoft voldeed het beste aan de eisen en wensen van de Eerste Kamer. De serviceverlening nemen we af via Strategisch Leveranciersmanagement (SLM) Microsoft Rijk (www.slmmicrosoftrijk.nl). Dat is conform het Rijkscloud-beleid.

NZa

Waarom besloot het bestuur van de NZa om haar infrastructuur onder te brengen bij Microsoft?
De NZa valt voor diensten en producten die zij van Microsoft afneemt onder de afspraken die de Rijksoverheid (SLM Rijk) met Microsoft heeft afgesloten. Er is voor Microsoft gekozen omdat de diensten en producten van Microsoft aansluiten bij de hoge eisen die de NZa stelt in tijden
waarin het werken steeds vaker op afstand plaatsvindt. De NZa treft passende technische- en organisatorische maatregelen volgens de relevante technische standaarden en richtlijnen. Verder maakt de NZa gebruik van diensten die gegevens opslaan binnen de Europese Economische Ruimte.

Is de aard van de communicatie te rijmen met het feit dat de Amerikaanse inlichtingendiensten het wettelijk recht hebben om die informatie op te vragen, ook al staat de informatie fysiek in Nederland?
De NZa gebruikt Microsoft Outlook voor (interne) zakelijke communicatie. Voor de uitwisseling van gevoelige gegevens worden andere, beveiligde, uitwisselprogramma's gebruikt. Daarbij merken wij op dat Microsoft op dit moment voldoet - en eerder ook voldeed - aan de eisen van (eerder geldende) adequaatheidsbesluiten. Het op dit moment geldende adequaatheidsbesluit, het EU-US Data Privacy Framework (DPF), houdt in dat de Europese Commissie heeft geoordeeld dat het beschermingsniveau van persoonsgegevens in de VS gelijkwaardig is aan dat van Europa. Mits het betreffende bedrijf in het DPF-register staat, voor Microsoft is dat het geval. Het DPF volgde op aanpassingen doorgevoerd in het rechtsstelsel van de VS. Eén van de aanpassingen is dat inlichtingendiensten alleen toegang tot gegevens mogen vorderen als dit 'noodzakelijk en proportioneel' is in het kader van de nationale veiligheid. De wettelijke vorderingsbevoegdheden van Amerikaanse inlichtingendiensten zijn daarmee nu van meer waarborgen voorzien dan in de vraagstelling wordt geschetst. Op de website van de de Autoriteit Persoonsgegevens - is meer informatie te vinden over de doorgifte van persoonsgegevens naar de VS. Zie bijvoorbeeld: https://www.autoriteitpersoonsgegevens.nl/themas/internationaal/doorgifte-binnen-en-buiten-de-eer/doorgifte-persoonsgegevens-naar-de-vs.

Is gebruik van een Nederlandse cloudprovider overwogen?
Er is gekozen voor diensten en producten die aansluiten bij de functionele, technische en beveiligingseisen die de NZa stelt aan het gebruik van een e-mailprogramma c.q. mailserver. Cloud is daarmee geen doel op zich, maar een gevolg van de keuze voor Microsoft. Er is vooralsnog geen geschikt Nederlands of Europees alternatief dat voldoet aan de eisen die de NZa stelt.

PBL

Voor zover wij weten is ons gebruik van een publieke clouddienst in lijn met het herziene Rijksbrede cloudbeleid van augustus 2022: https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2022Z15892&did=2022D33299. Nieuw beleid: cloud is toegestaan.

Wij hebben wel gekeken naar een Nederlandse cloudaanbieder, maar daarvan waren de gebruiksspecs aanzienlijk slechter tegen een vele malen hogere prijs.

Voor de zeldzame staatsgeheime documenten binnen onze organisatie, hebben we een apart analoog kanaal.

KVK

KVK maakt gebruik van onder meer O365 van Microsoft, maar heeft niet de gehele infrastructuur daarin ondergebracht.
De cloudstrategie van KVK bij het gebruik van O365 is in lijn met de richtlijnen van het Rijkscloudbeleid.

De derde vraag is volgens KVK niet relevant, met dien verstande dat KVK bij SaaS-diensten een risicoafweging maakt en dat de data van alle andere applicaties binnen private cloudomgevingen zijn ondergebracht in een tweetal datacenters in Nederland.

Nederlandse Vereniging van Banken
De NVB is groot voorstander van Europese autonomie en zou de ontwikkeling van een Europees alternatief toejuichen. Maar vooralsnog zijn die alternatieven er niet en zijn we aangewezen op Amerikaanse spelers voor clouddiensten.

Voor dat een bank besluit om een product of dienst te migreren naar de cloud maken zij hiervoor eerst een risicoanalyse waarbij expliciet rekening wordt gehouden met de wet- en regelgeving die van toepassing is. Als blijkt dat het betreffende product of dienst zich niet leent voor migratie naar de cloud dan zal de bank dit product of dienst vanuit het eigen datacentrum blijven aanbieden. Naast checks en balances binnen de bank houdt ook toezichthouder DNB scherp toezicht op dit soort processen.

Nationale Ombudsman

Waarom besloot de Nationale ombudsman van om zijn infrastructuur onder te brengen bij Microsoft?

Dit besluit hangt samen met de constatering dat IT in eigen beheer bij de Nationale ombudsman niet meer houdbaar was vanwege schaalgrootte, benodigde expertise en technische ontwikkelingen. Daarop is besloten om IT waar mogelijk uit te besteden, waaronder de e-mail infrastructuur.
Doordat we al werkten met Microsoft-producten, is ervoor gekozen om dit voort te zetten. Deze afweging is mede gemaakt op basis van functionele en technische functionaliteiten evenals vanuit financieel oogpunt. De Nationale ombudsman is zich bewust van de risico's rondom het gebruik van Cloud-diensten en is daarom ook aangesloten bij Strategisch Leveranciersmanagement Microsoft Rijk (SLM Microsoft Rijk), die Rijksbrede afspraken en inkoopvoorwaarden afsluit met Microsoft op het gebied van data en de toegang daartoe.

Is de aard van de communicatie te rijmen met het feit dat de Amerikaanse inlichtingendiensten het wettelijk recht hebben om die informatie op te vragen, ook al staat de informatie fysiek in Nederland?
De organisatie verwerkt geen geclassificeerde informatie en vertrouwt op de afspraken gemaakt tussen SLM Microsoft Rijk en Microsoft voor toegang tot opgeslagen data.

Is gebruik van een Nederlandse cloudprovider overwogen?
Nee. Het uitgangspunt bij de vernieuwing van bestaande technologie was om de bestaande integraties zoveel mogelijk intact te laten. Dit dus mede op basis van de afwegingen die wij ook in de beantwoording op vraag 1 noemen.

VEWIN (vereniging drinkwaterbedrijven)

De drinkwatersector neemt cybersecurity en digitale weerbaarheid uiterst serieus. Hiervoor werkt zij samen met o.a. het NCSC, het ministerie van Infrastructuur en Waterstaat en

collega-vitale aanbieders. Uit oogpunt van beveiliging doen wij geen uitspraken over nadere beleidskeuzes en/of beveiligingsmaatregelen.

Microsoft

Microsoft zet zich in voor de naleving van de AVG. Ter blijk van deze inzet heeft Microsoft de EU Data Boundary in het leven geroepen als extra maatregel. Daarmee garandeert Microsoft haar klanten dat gegevens die onder de EU Data Boundary vallen binnen de EU worden opgeslagen en verwerkt.

De CLOUD Act heeft specifiek betrekking op uitzonderlijke omstandigheden waarin een vermoeden van een ernstig misdrijf wordt vastgesteld waarvoor een opsporingsverzoek nodig is en kan ook gelden voor Europese bedrijven.

In dergelijke gevallen onderzoekt Microsoft elk juridisch verzoek van zowel EU- als niet-EU-wethandhavingsinstanties en voldoet het actief aan de AVG-principes. Waar mogelijk vecht Microsoft zowel EU- als niet-EU-verzoeken aan.

Google

Google belooft data van klanten desgevraagd binnen de EU te houden. Maar de extraterritoriale werking van de CLOUD Act maakt dat die belofte niet 100 procent waar is te maken. (...) Wat is jullie reactie daarop?
Google is committed to protecting the data our customers share with us, regardless of where our customers' information is processed. This means helping our customers meet stringent data protection requirements by offering industry-leading technical controls, contractual commitments, and risk assessment resources.
It's important to note that since this article was published (hier wordt het artikel bedoeld waarnaar je linkte in je vraag - RF) there have been important developments between the European Commission and US Government, resulting in an agreement to enhance privacy protections for EU data:

-On October 7, 2022 the US President signed an Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities, directing the steps that the US will take to implement its commitments under the European Union-U.S. Data Privacy Framework.
-On December 13, 2022 the European Commission issued a draft adequacy decision for the EU-U.S. Data Privacy Framework.
-On 10 July 2023, the European Commission adopted an adequacy decision for the EU-U.S. Data Privacy Framework.

Wat doet Google om te voorkomen dat niet-Europese partijen toegang hebben tot data van Europese klanten?
Google helps our customers meet stringent data protection requirements by offering industry-leading technical controls, contractual commitments, and products and services such as Google Distributed Cloud Hosted, Sovereign Controls and Assured Workloads.

For example, our Assured Workloads for the E.U product helps Google Cloud Platform (GCP) customers protect their data by allowing them to:

Store their data in their choice of E.U. Google Cloud region(s)
Ensure that only E.U. persons – located in the E.U. – have access to the data and provide customer support
Deploy cryptographic control for data access, including customer-managed encryption keys

In addition, our Google Workspace (including Workspace for Education) customers can choose to store their covered data in Europe. Additionally, with Client-Side Encryption, we offer customers direct control of encryption keys and the identity service they choose to access those keys. With Client-Side Encryption, customer data is indecipherable to Google. Client-Side Encryption is currently available in for Google Drive, Gmail, Calendar and Meet. Additionally, customers can also benefit by choosing third party solutions that offer similar encryption capabilities with select Google Workspace services.
Google is committed to ensuring the highest standards of privacy and security regardless of where the data is transferred, by offering industry-leading technical controls, contractual commitments, and risk assessment resources. We will continue to publish additional materials on our Cloud Privacy Resource Center, such as our whitepaper on international data transfers, to help our customers ensure compliant data transfer.

Google steunde de CLOUD Act, waar vooral uit Amerikaanse privacy-hoek veel kritiek op kwam. Waarom is dat?
Government engagement on a bilateral and multilateral level is critical for modernising laws and establishing rules on the production of electronic evidence across borders in a manner that respects international norms and sovereignty, and that resolves any potential conflicts of law. Google has supported these efforts and will continue to do so while protecting the privacy and security of our customers.

The Clarifying Lawful Overseas Use of Data (CLOUD) Act creates a mechanism by which a qualifying foreign government may enter into an executive agreement with the U.S., provided that the qualifying foreign government meets baseline privacy, due process, and human rights standards in the CLOUD Act.

It does not modify or relax the high standards that the U.S. government must meet before it can compel the production of communications content from a U.S. service provider; and it does not modify the DOJ's policy that prosecutors should request data from cloud customers directly, not from the customer's provider. Moreover, it does not require providers like Google to weaken their strict standards for reviewing government requests for data. Cloud providers can challenge a U.S. government data request on the basis of conflict of law related to a qualifying foreign government, provided the foreign government's law allows for a reciprocal right to challenge in the event of a request that conflicts with U.S. law.

Google was the first cloud provider to publish regular transparency reports on government requests for customer information, as well as requests for Google to remove content from publication.

The new Trans-Atlantic Data Privacy Framework also makes an important step towards further government negotiations of CLOUD Act Agreements — including between the US and EU — as vehicles for surveillance reform - which we have been advocating for in response to governments and customer requests, among other things, in Europe. We welcome the ongoing negotiations for a US-EU e-evidence exchange agreement to facilitate the production of electronic evidence across borders in a manner that avoids potential conflicts of law and protects the privacy and security of customers and individuals.

Amazon

V1 & V2
De Cloud Act geeft handhavingsinstanties geen toegang tot serviceproviders en geeft ze ook niet de middelen om rechtstreeks toegang te krijgen tot servers of klantgegevens. De Cloud Act biedt een streng mechanisme waarmee wetshandhavers tijdens een strafrechtelijk onderzoek naar een Amerikaanse rechtbank kunnen gaan om gegevens op te vragen bij serviceproviders. Om een formeel verzoek voor data in te kunnen dienen, moet eerst worden voldaan aan de strenge wettelijke normen die worden gesteld aan het verkrijgen van een bevelschrift van een Amerikaanse rechtbank. In de halfjaarlijkse transparantieverslagen van AWS wordt opgemerkt dat er geen gegevensverzoeken aan AWS zijn gedaan die hebben geleid tot openbaarmaking van buiten de VS opgeslagen bedrijfs- of overheidsgegevens aan de Amerikaanse overheid. Deze verklaring werd in 2020 toegevoegd aan het transparantieverslag en is sindsdien elke zes maanden opnieuw bevestigd.

AWS zet zich volledig in voor de bescherming van klantgegevens. We blijven klanten helpen om met succes te voldoen aan veranderende Europese wetten en normen en om de hoogste niveaus van beveiliging, privacy en veerkracht te bereiken. AWS biedt uitgebreide technische, operationele en contractuele maatregelen om content van klanten te beschermen en over te dragen buiten Europa in overeenstemming met de General Data Protection Regulation (GDPR). Klanten kunnen er ook voor kiezen om hun content in de Europese Unie op te slaan door een of meer van onze regio's in Frankrijk, Duitsland, Ierland, Italië, Zweden en Spanje te selecteren, met het vertrouwen dat hun gegevens in de door hen geselecteerde AWS-regio blijven.
Daarnaast kunnen klanten een geavanceerde set toegangs-, versleutelings- en logboekfuncties gebruiken om volledige controle over hun inhoud te behouden. Versleutelde content is onbruikbaar zonder de toepasselijke ontsleutelingscodes.

In 2023 onderzocht het Nederlandse Ministerie van Justitie de risico's van gegevensbescherming en -overdracht bij het gebruik van AWS-diensten. De uitkomst van deze Data Protection Impact Assessment (DPIA) is dat er geen bekende hoge risico's zijn als Nederlandse overheidsorganisaties de aanbevolen mitigerende maatregelen in de DPIA volgen.

V3
Amazon Web Services was geen ondertekenaar van de openbare brief van technologiebedrijven aan het Amerikaanse Congres over de Cloud Act. We hebben het punt

gemaakt dat de Cloud Act in ieder geval het recht van cloudproviders erkent om verzoeken aan te vechten die in strijd zijn met de wetten of nationale belangen van een ander land en vereist dat overheden lokale rechtsregels respecteren.